ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

بسم الله الرحمن الرحيم

أخواني قد جمعت لكـم عدد من المـواضيـع بعضـها قمت بكتابتـه والبعض منها منقول وهو قـرابـة((الـثــلاثــيـن مـــوضـــوع)) والأفـضـل وضــعـهـا وحـفـظــهـا فـي الأرشـيـف

الموضوع الأول : إقفال 99% من منافذ جهازك أمام الهكرز

1- اذهب الى قائمه ابدأ

2- start + run

3- اكتب في مربع الكتابه التالي command.com

3- ستظهر لك نافذه اكتب بها التالى host ping

4- اضغط enter

وانتظر قليلاً ثم اكتب ping port

ثم اضغط على enter

5- انتظر ثم اكتب التالى ping port 1027

ثم اضغط على enter

6- انتظر ثم اكتب التالى ping proxy

ثم اضغط enter

7- انتظر ثم اكتب التالى ping port

ثم اضغط enter

والان تم تقفيل 99% من منافذ جهازك امام الهكرز

الموضوع الثاني : معرفة من قام بحظرك بدون أي برنامج

هام لمستخدمي الهوتميل الان باستطاعتك معرفة من قام بحظرك؟

من السهل معرفة من قام بحذفك من أصدقائك في ماسنجر الهوتميل وذلك بالذهاب إلى أدوات في القائمة الرئيسية ثم خيارات ثم للخصوصية وتقوم بتحديد صديقك في الماسنجر وبالضغط على زر الفأرة الأيمن تشاهد كلمة حذف فإذا كانت مفعلة معناه أن صديقك في الماسنجر قد قام بحذفك.

ولكن الجديد هنا هو أنك تستطيع إن تعرف أن كان يعمل حظر لك بحيث يستطيع مشاهدتك أثناء دخولك على الماسنجر وذلك باتباع الخطوات التالية :

1 اذهب إلى ابدأ Start ثم إلى تشغيل Run وفي سطر الأوامر أكتب هذا الأمرregedit

تفتح لك ويندوز Registry Editor أختر المجلد الثاني HKEY_CURRENT_USER

2 من HKEY_CURRENT_USER أختر Software ثم Microsoft واختر Messenger Service ثم List Cache ثم NET. Messenger Service.

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

3 سوف يظهر لك العديد من الملفات في الجهة اليمنى من **Registry Editor** وهذه الملفات مقسمة إلى عدة أنواع وكل ملف منها يحتوي على معلومات خاصة بأصدقاءالماسنجر لديك

النوع الأول من الملفات (**Allow**) : يحتوي هذا النوع من الملفات على معلومات صديقك الموجود في الماسنجر والذي أنت معه على اتصال بدون حذف أو حظر بحيث تستطيع رؤيته عند دخولكما للماسنجرسويا

النوع الثاني من الملفات (**Block**) : يحتوي هذا النوع من الملفات على معلومات صديقك الذي قام بحظرك أو أنت قمت بحظره في الوقت الحالي

النوع الثالث من الملفات (**Contact**) : يحتوي هذا النوع من الملفات على معلومات صديقك الذي طلبت منه إضافتك على الماسنجر ولم يستقبل إضافتك حتى الآن

النوع الرابع من الملفات (**Reverse**) : يحتوي هذا النوع من الملفات على معلومات صديقك في الماسنجر الذي سبق وأن عمل لك حظراً وأعادك إلى القائمة لديه أو أنت قمت بحظره وأعدته الى القائمةلديك . وبصفة عامة عند نقرك مرتين على أي من الملفات السابقة سوف يظهر لك العديدمن المعلومات منها بريد صديقك وغيرها من المعلومات الرقمية

<u>الموضوع الثالث : 29 طريقه للحفاظ على إيميلك</u>

1 - ان تكون كلمة المرور طويلة جدا ، لأن البعض يجعل خانات كلمة المرور عبارة عن خمس او سبع خانات والافضل ان تجعلها اكثر من عشرين خانة

2 - ان تحتوي كلمة المرور على خليط من الرموز ، الأرقام و الحروف مثال 19
MYO~QM/+^%BO*ZP37

3 - ان لا تضع كلمة المرور بسيطة الادخال على لوحة المفاتيح حتى وان اشتملة على النقطتين السابقتين 1 - 2 لأن البعض يجعل كلمة المرور بهذا الشكل **QWERTYUIOP123*&^%$#**
لا حظوا ادخلنا الرموز اولا بالترتيب لأنها في الجزء الاعلى من لوحة المفاتيح ثم ادخلنا الاحرف التي اسفل من الرموز في لوحة المفاتيح ايضا بالترتيب ثم ادخلنا الارقام مرتبة ، والافضل التنقل في جميع اجزاء لوحة المفاتيح بشكل عشوائي حتى يصعب تخمينا او قد يتمكن شخص من الحصول على كلمة المرور بضربة حظ !

4 - ان لا تكون كلمة المرور عبارة عن ارقام تسلسلية او ارقام عشوائية قد تراها انت صعبة لكن سهلة عندما يكون هناك برنامج لأنتاج الارقام سواء تسلسلية او عشوائية مهما طالة الخانات . والبعض يستخدم ارقام تسلسلية مثل 123456789 او 1223334444 او 102030405060 والكثير من هذه الامثلة والبعض يستخدم كلمات مرور بهذا الشكل بكل ثقه !

5 - ان تكون كلمة المرور بعيدة جدا عن أي معلومة حقيقية تخصك مثل رقم الهاتف اسمك اسم المدينة الدولة التي تسكنها تاريخ ميلادك لأن البعض يجعل كلمة المرور بأسم الدولة او المدينة ثم يتبعها بتاريخ الميلاد وهكذا وايضا ان تبعدها عن أي معلومة معروفه عنك في منتدى تشارك فيه حتى ولو كانت تلك المعلومة تخص اسمك المستعار

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

6 - ان تكون كلمة المرور بعيدة عن الأسماء المشهورة وايضا الأجنبية مثل اسم لاعب او اسم مغني لأن مثل هذه الكلمات تكون قريبة للفكر والتخمين اكثر ولأن هناك برامج تعتمد في عملها على ملفات بها كلمات مرور اجنبية تقوم بتجربتها على البريد ، ايضا تسمح هذه البرامج بأضافة كلمات مرور اخرى ضمن قائمتها او قد يخصص قائمة لهذا البريد بهدف سرقته فيضع جميع الكلمات التي يتوقعها

7 - ان تثق في الشخص الذي تراسله لأنه بعد فترة من الزمن من الاخذ والعطاء يستطيع جمع معلومات عنك قد تفيده في كشف كلمة المرور

8 - ان لاتجعل كلمة المرور هي اسم مُرسل البريد لأنها قد تفيد حتى وأن اتبعتها بأضافة بسيطة ليست معروفه . لأن البعض يكون اسمه **snowfall** الذي ادرجه عند تسجيل البريد فيضيف اسم البريد مع اسم الُمرسل وتكون كلمة المرور بهذا الشكل **Snowfallsnowfallitgo or snowfallsnowfallitgoyahoocom**

9 - تغيير كلمة المرور بين فترة وأخرى لأنه ربما يكون هناك شخص استولى بالفعل على البريد لكن لم يغير كلمة المرور ينتظر ان تصل لبريدك رسائل مهمه او قد يتصف بالجاسوسية يريد ان يتعرف عليك اكثر ! ولتأ كد ان الرسالة لم تقرء تجد شريط عنوان الرسالة نشط واذا قرءة الرسالة تجد تغير في لون عنوان الرسالة أي غير نشط

10 - ان تكتفي ببريد واحد او اثنان وان تجعل لكل واحد منهما كلمة مرور مختلفة لأن البعض من كثرة ما يملك من حسابات بريدية يتكاسل ويجعل لها كلمة مرور واحدة فأذا سُرِق أي بريد منها سوف يفقد بقيتها

11 - اذا كنت تملك كلمات مرور صعبة التذكر لطولها او لأشتمالها على خليط من الرموز ، الارقام والحروف وصعبة الحفظ والتذكر سواء كانت لبريد لبطاقة بنكية او لمنتدى لا تجعل لها ملف خاص داخل الجهاز أكتبها في ورقة خارجية والصقها بالقرب من الجهاز او اكتبها في نوتة الأرقام الهاتفيه اكتبها في مكان آمن بعيدا عن الجهاز

12 - اذا كنت تشارك بمنتدى اجعل بريدك المعروف لأعضاء المنتدى وزواره للأختبار فقط أي لا تجعله البريد الأساسي اوالشخصي الذي تستقبل فيه معلومات خاصه وحقيقية عنك مثل ان تراسل زوجتك او اشخاص بينك وبينهم امور شخصية على هذا البريد

13 - يجب ان تكون حذر جدا عند استخدام الماسينجر وان تثق في الشخص الذي تتحدث معه لأنه لو طلب منك ان تتحدث معه بالصوت يستطيع ان يحدد رقم الأي بي الخاص بك أثناء التحادث ويستخدم بعد ذلك برنامج كراكرز في الوصول لجهازك مباشرة وهناك الكثير فقد السيطرة على بريده بعد استخدامه للماسينجر وحتى وان كانت المحادثة نصية ، ايضا البعض يدخل لحسابه البريدي من خلال الماسينجر ويطلب من الماسنجر ان يحفظ كلمة المرور والأفضل الدخول للبريد من الموقع ، ايضا هناك برامج متخصصه في الحصول على كلمات المرور وتعمل هذه البرامج اثناء استخدام الماسينجر!

14 - الابتعاد عن مواقع البريد المشهورة وحاول بقدر المستطاع ان تأخذ لك حساب بريدي في مواقع ليست مشهورة لأن معظم الطرق والبرامج المستخدمة والتجارب في الحصول على كلمات المرور جميعها واغلبها موجهه لهذه المواقع

مثل موقع الهوت ميل وهذا ملاحظ وكثير ما نسمع من فقد كلمة مرور حسابه البريدي في هذا الموقع وايضا بريد الياهوه مع انها تقدم خدمات قد لا نجدها في مواقع أخرى و مستوى الأمن بها عالي ولأفضل الابتعاد عنها هذا من وجهة نظري

سيف علي حسن الدار
+967/ 771323146-735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

15 - الأبتعاد عن المواقع الشخصية لأن بعض منها تقدم مجال من خلالها أي من خلال الصفحة لدخول الي حساب بريدك مثل بريد الهوت ميل اوالياهوه او أي بريد آخر ونجد فيها حقل لأسم حساب البريد وحقل لكلمة المرور وفي الحقيقة ما هي إلا طريقة للحصول على كلمة المرور فعندما تريد الدخول لحسابك من خلال هذا الموقع تُرسل معلوماتك لصاحب هذه الصفحة وتقع في فخ ولذلك لا تدخل لبريدك إلا من موقعه الاصلي

16 - تعطيل تشغيل خاصية جافا سكربت لأنها تستخدم في اعادة ادخال معلوماتك من اسم الحساب وكلمة المرور لتصل للمستفيد وهي رمز يدرج في الرسالة وعند فتح هذه الرسالة تظهر لك مطالبة بأعادة ادخال معلومات بريدك من اسم الحساب وكلمة مرور وبعد ذلك توجه معلوماتك من اسم الحساب وكلمة مرور للمستفيد وهي تنطبق على أي بريد وللهروب من هذه الرسالة عليك اعادة ادخال بيناتك من حقل الموقع الاصلي وليس من حقل الرسالة الوهمية

17- لا تجعل جهاز الكمبيوتر يستخدم خاصية الإكمال التلقائي لأن هذه الخاصية عند استخدامها تحتفظ بجميع كلمات المرور التي ادخلتها سواء في بريد او منتدى او بطاقة بنكية داخل الجهاز و الاغلبية منكم قد لاحظ عند كتابته اول حرف من اسم حسابه في البريد او في المنتدى يظهر الاسم مباشرة دون الحاجة لأكمال اسم الحساب وايضا عند ادخال كلمة المرور تظهر كلمة المرور مباشرة في شكل نجوم وهذا دليل على ان اسم حسابك وكلمة المرور يحتفظ بها الجهاز فقد يسيطر على جهازك كركرز ومن المعروف ان معظم برامج الكركرز يوجد بها امر مخصص فقط للحصول على كلمات المرور واسماء الحسابات المخزنة في الجهاز نتيجة خاصية الاكمال التلقائي ولتعطيل خاصية الإكمال التلقائي وهذه نقطة مهمة جدا من متصفح الأكسبلور نختار منه

أدوات- خيارات إنترنت – محتوى - إكمال تلقائي

أزل جميع علامات صح من الخيارات الموجودة اسفل من هذه الجملة

استخدام الإكمال التلقائي لـ

عنوين ويب . ازل علامة صح

النماذج . ازل علامة صح

اسماء المستخدم وكلمات المرور في النماذج. ازل علامة صح

المطالبة بحفظ كلمات المرور. ازل علامة صح

اضغط على زر مسح كلمات المرور

اضغط على زر مسح النماذج

ثم موافق .

يجب الأنتباه بعد هذه الاعدادات لأنه سوف تظهر لك رسالة عند الدخول لأي حساب تخبرك هل تريد استخدام الإكمال التلقائي اختر لا . واحتمال كبير ان تستمر معك ، ايضا الأنتباه للخيار وغالبا ما نراه في مواقع البريد وبرنامج الماسينجر وهو تذكر كلمة المرور واسم الحساب على هذا الجهاز لا تضع علامة صح على هذا الخيار

18 - الأبتعاد عن استخدام أي طريقة لأستعادة كلمة المرور التي فقدتها لأنه ربما تكون ضحية للمرة الثانية وعن البرامج المتخصصه في هذا المجال لأن اغلبها عبارة عن تروجين قد تسيء استخدامها وتقع في فخها و الابتعاد ايضا عمن يقول انه يستطيع اعادة كلمة المرور والابتعاد عن المواقع وخصوصا الشخصية التي تدعي انها تعيد كلمة المرور التي فقدتها

19 - دائما وابدا عند الانتهاء من تصفح بريدك وقرائت الرسائل اختر الامر خروج من حساب البريد **Sign Out** لأنه عند محاولة الرجوع لصفحة البريد بعد ذلك يتطلب منك ان تدخل كلمة المرور وهذه النقطه مهمة جدا خصوصا لزوار مقاهي الانترنت لأنه لو استخدم شخص آخر الجهاز يستطيع الدخول إلي بريدك

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

20 - لأبتعاد عن ارسال روابط المواضيع من خلال الماسينجر وهنا اتكلم للحفاظ على حساب الأشتراك بالمنتديات لأنه عند ارسال رابط لموضوع وانت بالفعل داخل المنتدى بحساب اشتراكك يستطيع مستقبل هذا الرابط ان يضيف مشاركات ومواضيع تحمل اسمك في هذا المنتدى وهي نتيجه لأتصالكم ببعض في نفس اللحظة كما لو كنتم في جهاز واحد ولذلك يجب الخروج الرسمي من المنتدى واكثر المنتديات يوجد بها خيار الخروج لأن وحتى وإن حاول الشخص الذي معك على الماسينجر في نفس اللحظة اضافة موضوع او مشاركة تحمل اسمك بعد استخدامك امر الخروج من المنتدى سوف لن يستطيع ابدا فعل أي شيء لأن الموقع سوف يتطلب منه اسم المستخدم وكلمة المرور ، وكثير ما نرى مثل هذه المواقف فنرجوا الانتباه ، وايضا هذه النقطة ينتبه لها زوار مقاهي الانترنت . وهذا برنامج يقوم بمسح ملفات الكوكيز تلقائيا من الجهاز والتي تستخدمها معظم المنتديات في تصفح الموقع دون الحاجه للخروج الرسمي من الموقع وله مهام اخرى اسم البرنامج : **Surf Version 1.50 Ghost**

21 - ان تتجنب فتح المرفقات الأتيه من طرف مجهول ولو كانت من صديق من يظمن ! لأنها قد تكون عبارة عن تروجين وما ان تفتحها حتى يثبت التروجين بجهازك ويوجد الكثير من هذا التروجين مخصص فقط للبريد للحصول على كلمة المرور وتوجيهها لبريد المستفيد مباشرة ومنها لأوضح لكم خطورتها يعمل على حفظ أي عملية ادخال تمت على لوحة المفاتيح لأي حساب حتى وان تعطلة خاصية الإكمال التلقائي ! وقد لا يكتشفها برنامج الحماية لأنها ربما تكون مدمجه مع ملف حماية !

22 - ان تثق في المنتدى الذي تشارك فيه لأن البعض يجعل كلمة مرور البريد هي كلمة مرور حسابه في المنتدى او يكون المسؤل عن المنتدى غير آمن .
وهذا وللأسف منتشر بين بعض المنتديات العربية

23 - عند استيلاء شخص على بريدك ويوجد رسائل مهمة جدا لا تريد ان يطلع عليها مهما كلف الامر من وجهة نظري عليك بستخدام برنامج تدمير البريد لأن مهمة هذا البرنامج هي ارسائل الاف الرسائل للبريد وبذلك يصعب ملاحظة رسائلك المهمة مع الكم الهائل من رسائل تدمير البريد ولا ننسى وضع عناوين مختلف لكل مجموعة رسائل او ان تجعلها بنفس عناوين الرسائل التي لا تريده ان يقرئها

24 - ابتعد عن ارسال رسالة تتضمن سب او شتم للشخص الذي استولى على بريدك ولا تظهر الاهمية له لأنه ربما يزداد تمسكا به وحاول بعد فتره ان تتملك عاطفة هذا الشخص برسائل من يدري قد يعفوا عن بريدك !

25 - عند تسجيلك لحساب بريدي لأول مرة لا تكتب معلوماتك الحقيقية في طلب تسجيل البريد فرضا تسكن بالسعودية اختر اسكن بالهند بمدينة كلكتا الأسم جاتندر أي اسم المهم لا تكن معلومات حقيقية . راجع الفقرة 5 - 7- 8

26 - حاول بقدر المستطاع ان تحتفظ بصفحة المعلومات الشخصية لحساب بريدك في **Floppy** قرص مرن وليس داخل الجهاز لأن الكثير ينسى معلومات التسجيل هذه والتي تتضمن السؤال السري لتفيده بعد ذلك اذا فقد كلمة المرور في مراسلة المسؤل عن موقع البريد لأستعادتها

27 - التأكد من بريد المسؤل عن الموقع اذا اردة ارسال بياناتك لأستعادة كلمة المرور وتجد البريد الاصلي في صفحة المساعدة من البريد

28 - الكثير منا عند ادخال بياناته في طلب تسجيل بمنتدى او بريد لا بد من ان يضع بريده ضمن متطلبات التسجيل و لكي يستقبل عليه معلومات التسجيل ومن ضمنها كلمات المرور ولذلك من الافضل ان تخصص بريد لهذا الشئن بذلك تفقد البريد ولا تفقد الكثير !

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

الموضوع الرابع : أشكـال الإختـراق

يتعرض مستخدم الانترنت لعدة أشكال من الاختراق بعضها تقني وبعضها بشري.
الاختراق البشري يعتمد على مدى فطنة المستخدم وثقته بالاخرين والسماح لهم بمعرفة خصوصياته.
الاختراق التقني مرتبط بثلاث أنواع من الاختراق،
(1) نظامي من السلطات بشكل معلن أو غير معلن، وكل الدول تقريبا فيها اختراق من هذا النوع بما فيها أمريكا ودول أوربا.
(2) اختراق مباشر ولحظي من قبل الهاكرز يجد فيه المخترق ثغرة في منافذ اتصال المستخدم ويستطيع التجول بين ملفات وبرامج المستخدم ونسخها أو قرائتها أو تخريب جهاز المستخدم أو عمل أي شي آخر.
(3) اختراق بفيروسات التجسس وهو أكثر خطورة من السابق حيث يتمكن الهاكر من تثبيت فيروس تجسس في جهاز المستخدم ويقوم الفيروس بإرسال معلومات حسب الطريقة التي برمج بها.

التصفح

مع أن مزودي الخدمة يستطيعون نظريا أن يتتبعوا المستخدمين ألا أنه يكاد يستحيل تطبيق هذه الخدمة بشكل دوري على الجميع. وسبب عدم تتبع الدولة هو اكتشافها أن هذا التتبع غير عملي ولذلك وصلت السلطات المختصة إلى استنتاج في وقت مبكر أن تتخلىعن متابعة الناس بخصوص التصفح المجرد.

إنزال الملفات

هناك مواقع كثيرة في الانترنت تعرض ملفات من أنواع مختلفة مثل برامج مجانية أو فلاشات أو كتب أو صور أو أمور أخرى. وما لم تكن هذه المواقع معروفة وموثوقة فيفضل أن لا يتم تنزيل ملفات منها لأن بعضها مليء بفيروسات التجسس.

المشاركة في المواقع

يعتمد الأمان في المشاركة في بعض المواقع (المنتديات وماشابهها) على مدى أمن الموقع وأختراقه من قبل بعض الجهات أو الهاكرز...

البريد الالكتروني

(1) البريد نفسه يفضل أن لا يعلن وإذا أعلن في المنتديات أو غيرها لا يستخدم المعلن إلا لأمور رسمية لها علاقة بالمنتديات وينشأ بريد آخر خاص للاستخدام الخاص.
(2) يفضل أن تستخدم باسوورد طويلة وصعبة وتغير بين فينة وأخرى.
(3) يفضل أن لا تبقى الرسائل في حافظة البريد (صندوق الوارد) ويحرص المستخدم على حذفه دائما.
(4) يفضل أن لا يراسل المستخدم أي جهة لا يعرفها ولا يقبل أي رسالة وخاصة الرسائل المحملة بالملفات ويبادر بحذفها قبل فتحها.
(5) يتجنب المستخدم مطلقا استخدام إسمه الحقيقي أو وضع أي معلومات في تسجيل البريد تدل على شخصيته إلا أن يكون البريد معلنا ومعروفا لأسباب تخص نوع العمل.

الماسنجر

شاع استخدام الماسنجر بشكل كبير جدا وأصبح أداة فعالة للمخترقين في التعرف على أسرار المستخدمين. وللأمان من أخطار الماسنجر ننصح بالخطوات التالية:
(1) إذا اضطر المستخدم أن يعلن ماسنجرا معينا فعليه أن يفترض أن هذا المعلن عرضة للاختراق ويحرص على اقتناء ماسنجر آخر غير معلن.
(2) يتجنب مستخدم المسانجر قبول إضافة أي شخص أو جهة لا يعرفها لأن فرصة الاختراق بعد الإضافة تزداد وتزداد

أكثر بعد الدخول في محادثة.

(3) يتجنب مستخدم الماسنجر قبول نقل الملفات من الماسنجر لأن نقل الملف من منفذ المسانجر لا يمر بعملية الكشف على الفيروسات التي تتم في الانترنت. وينطبق هذا حتى على الأشخاص الذين يثق بهم لأن الشخص الموثوق به قد يكون جهازه مخترق أو مصاب بالفيروسات وهو لا يعلم.

(4) يتجنب مستخدم الماسنجر الدخول في حديث صوتي أو تشغيل كاميرا خاصة مع من لا يعرفهم لأن هذه الخدمة تفتح ثغرات لا تستطيع برامج الحماية إقفالها.

(5) يتجنب المستخدم مطلقا استخدام إسمه الحقيقي أو وضع أي معلومات في الماسنجر تدل على شخصيته. كما يتجنب الإشارة لأي جانب من شخصيته في محادثاته لمن لا يعرف.

(6) يجب التنبه إلى أن إسم الماسنجر لا يكفي للحكم على شخصية المقابل بل يجب التنبه للبريد نفسه لأن البريد هو الذي يحدد شخصية الماسنجر.

(7) يتجنب المستخدم الضغط على الروابط التي توضع له في المسنجر لأنه بالإمكان معرفة الكثير من المعلومات عن جهازك من خلال ضغطك على أي رابط.

البال توك

في الجملة يسري على البال توك ما يسري على الماسنجر ما عدا النقاط التالية:

(1) بالنسبة للغرف العامة لا يوجد أي خطر من مجرد حضور هذه الغرف وكل ما يقال عن ذلك هو لتخويف الناس من المشاركة في البال توك.

(2) بالنسبة للمشاركة في الحديث في الغرف العامة يعتمد الأمر على معرفة صوت المتكلم فقط وليس له علاقة بما يقال عن معرفة الأي بي.

(3) بالنسبة للغرف الخاصة لا تزال التكنولوجيا فيها غير كاملة ويمكن اختراق هذه الغرف إذا كانت واضحة في القائمة فلذلك ينصح من يستخدم هذه الغرف بأن يضعها في قائمة غرف لغات غير العربية.

(4) بالنسبة للحديث المباشر على شكل شبيه بالهاتف في البال توك لا تزال هناك فيه بعض الثغرات ونسبة الأمان فيه ليست كاملة.

(5) توجد في البال توك مشكلة تخفى على بعض الناس هي إمكانية أن يظهر المستخدم بإسم يشبه تماما إسم شخص آخر فينخدع المقابل به

ثقافة الحماية

ينبغي على كل مستخدم حريص على سلامة معلوماته الشخصية وعلى جهازه وعلى اتصالاته ومراسلاته أن يتعلم ولو شيئا بسيطا عن طرق الاختراق مثلما بيناه أعلاه. ومع كثرة المخربين والفاسدين والجواسيس الذين يتبعون جهات مختلفة فينبغي أن يكون الأصل في التعامل مع الآخرين في الانترنت هو الحذر وعدم التبرع بأي معلومة تدل على الشخصية أو السكن أو تفاصيل عن نوع العمل أو نوع الدراسة مما يؤدي للتعرف على الشخصية. وينبغي أن يمتنع مستخدم البريد أو المسنجر أو البال توك من إعلان إسمه أو تسهيل وصول المستخدمين الآخرين إليه إلا إذا كانت طبيعة عمله تستدعي ذلك.

برامج الحماية المباشرة

برامج الحماية المباشرة من الاختراق اللحظي المباشر كثيرة والشركات التي تنتجها بينها تنافس كبير في قوة الحماية وكل مستخدم يفضل نوعا يروق له من البرامج. لكن ربما كان من أكثر البرامج شعبية في هذا الجانب هو الزون الارم الذي قد يعتبر أسهل استخداما من غيره من البرامج وأثبت قدرته على الحماية الفعالة من الاختراق المباشر. من البرامج الأخرى برنامج انترنت سيكوريتي التابع لمجموعة النورتن ولا يمنع أن يركب المستخدم كلا البرنامجين.

سيف علي حسن الدار
+967/ 771323146-735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

الحماية من الفيروسات

يمكن تنفيذها بالبرامج المضادة للفيروسات والتي من أشهرها برنامج النورتن أنتي فيروس وكذلك النسخ الجديدة من الزون الآرم. ولمن لا يستطيع الحصول على النورتن بإمكانه أن يحصل على برامج حماية فعالة وقوية يمكن إنزالها من مواقع في الانترنت (مثل البي سي سيلين) تعطي نسخ مجانية لمدد محدودة.

التحديث المستمر ومعرفة كيفية إعداد برامج الحماية.

يفضل أن يجري مستخدم الانترنت تحديثا دوريا لبرامج الحماية كما يفضل أن يغير الباس وورد التي يستخدمها في البريد والماسنجر والبال توك كما أننا ننبه إلى ضرورة إعداد برامج الحماية الإعداد المناسب للحصول على أقصى درجات الأمان

الموضوع الخامس : كيفية التخلص من صوت الموديوم

اليكم هذه الطريقة للتخلص من صوت المودم اثناء الاتصال بالانترنت معلومة وجدتها في احدى المجلات فحبيت ان انقلها لكم حتى تريحوا اذانكم من ضجيج المودم .

عندما تتصل بالإنترنت ، فإن الجهاز يصدر عدداً من الأصوات المتلاحقة التي تدل على الاتصال ثم الدخول إلى الإنترنت ، لكن في كثير من الأحيان فإن هذه الأصوات المتداخلة تكون مزعجة إلىحد ما .. لجعل المودم لا يصدر أي صوت ادخل إلى القائمة Control panal من الأمر Start ، ثم اختر Modem ، واختر نوع المودم الذي تملكه ثم انقر على P roerties ، نت صندوق الحوار الذي يظهر أمامك اختر Modem ثم عدل مستوى الصوت إلى الحد الذي تريده بجانب الأمر Speaker volume

ويفضل إعادة تشغيل الجهاز بعد عمل الخطوات السابق

الموضوع السادس : معلومات عن مشغل الإسطوانات الليزر

مشغل اسطوانات الليزر CD Drive وهو أحد وسائل التخزين التي حظيت بانتشار واسع في الوقت الحالي، ويعد تطوراً لوسائل التخزين التقليدية مثل الديسكات المرنة ولكنه يتميز عنها بكبر سعته التخزينية (من 650 ميجابيت إلي 700 ميجابايت) وذلك للاسطوانات العادية وتصل إلي 7 جيجابايت لاسطوانات ال DVD في حين ان التكلفة متساوية تقريبا، بجانب مقدرة هذ الاسطوانات علي تخزين الموسيقي للعمل علي أجهزة الكاسيت العادية التي تحتوي علي قارئ اسطوانات. ولكل ما سبق فقد اصبحت الاسطوانات هي وسيلة التخزين الرئيسية والأكثر استخداماً في وقتنا الحاضر.

وظيفة مشغل الأسطوانات الليزر هي إيجاد وقراءة المعلومات المخزنة علي الأسطوانة علي هيئة أجزاء بارزة أو

مرتفعة، ونظرا لصغر حجم هذه الأجزاء يجب أن يكون هذا المشغل دقيقاً جدّا في عمله. ولكي نتفهم طبيعة عمل المشغل بشكل سليم فلابدّ من التعرض بشكل سريع لطبيعة الإسطوانة نفسها.. فالاسطوانه المدمجة عبارة عنّ قطعة بسيطة من البلاستيك، يبلغ سمكها حوالي 100/4 من البوصة أي ما يعادل حوالي 1.2 مم و قطرها يساوي حوالي 12 سم، ويمكن للأسطوانه أن تحمل MB650 من البيانات أو ما يعادل 74 دقيقة وأصبح منها أنواع يمكنها تحميل MB700، أو 80 دقيقة، وتتكون معظم الاسطوانات من مادة carbonate plastic Clear poly المصبوب بطريقة

الحقن وأثناء التصنيع يضغط علي هذا البلاستيك بصدامات ميكروسكوبية، مرتبة بجانب بعضها بحيث تشكل مسار بيانات مستمراً لولبي الشكل عندما يتم الضغط علي البلاستيك بها. ويبلغ عرض مسار البيانات هذا حوالي 0.5 ميكرون والمسافة الفاصلة بين المسار والمسار المجاور له تكون حوالي 1.6 ميكرون (الميكرون = 1/ 1000000 م) ، والأجزاء البارزة التي تكون المسار، يبلغ عرض كل جزء منها نفس عرض المسار أي 0.5 ميكرون و طوله علي الأقل 0.83 ميكرون و ارتفاعه يساوي 125 نانوميتر (النانوميتر = 1/ 1000000000 م) هذه الأبعاد الدقيقه جدا تجعل المسار اللولبي الذي علي الاسطوانه طويل جدا، لدرجة انه إذا تخيلنا أنه يمكننا أن نرفعه من علي الاسطوانه و نفرده فسيتكون لدينا خط طوله حوالي 5 كم (3.5 ميل) و عرضه 0.5 ميكرون !! وعندما تنتهي عملية صب البلاستيك وضغطه بالصدامات الميكروسكوبية، يتم رش طبقة رفيعة عاكسة من مادة الألمنيوم **Aluminum** علي الأسطوانة. بعد ذلك يتم وضع طبقة رفيعة من مادة الأكريلك**Acrylic** علي طبقة الألمنيوم لكي تحميها. وأخيرا يتم طباعة الملصق**Label** الذي يتم كتابة محتويات الاسطوانات عليه علي طبقة الاكريلك .والآن مما يتكون هذا القارئ ؟ يتكون القارئ من ثلاثة أجزاء رئيسية :

1- موتور**Drive motor** يقوم بتدوير الأسطوانة، ويتم ضبط سرعة دورانه من 200 لفة بالدقيقة إلي 500 لفة بالدقيقة تبعا لمكان المسار الذي تتم قراءته حاليا علي الاسطوانة.

2- منظومة الليزر والعدسات **Laser and a lens system** تتركز وظيفتها في قراءة البيانات من الأسطوانة.

3- منظومة التتبع **Tracking mechanism** وظيفتها هي تحريك منظومة الليزر حتي يتمكن شعاع الليزر من تتبع المسار اللولبي، ويجب أن تكون دقة هذه المنظومة عالية جدا حتي تتمكن من تحريك منظومة الليزر بأبعاد تصل للميكرون. يتم داخل قارئ الاسطوانات تحويل البيانات المخزنة علي الأسطوانة - غير المفهومة - إلي مجموعات من البيانات التي يمكن التعامل معها ثم إرسالها إما إلي **DAC (Digital to analoue converter)** في حالة ما إذا كانت **Audio CD** ، أو إلي كمبيوتر إذا كانت**Data CD** . وتتمثل الوظيفة الرئيسية لمشغل الأسطوانات في تركيز شعاع الليزر علي مسار البيانات، عندما يصل شعاع الليزر إلي الأسطوانة يمر من خلال طبقة البلاستيك ثم ينعكس عندما يصطدم بطبقة الألمنيوم و يذهب الشعاع المنعكس إلي خلية الكتروضوئية وظيفتها الإحساس بالتغيير في الضوء، وهنا لدينا حالتان إما أن يصطدم شعاع الليزر بجزء مرتفع فيقع -عندما ينعكس- علي خلية الكترو-ضوئية و يمكن تمثيل هذه الحالة ب (1)، أو يصطدم شعاع الليزر بجزء منخفض فلا يقع عندما ينعكس علي الخلية الكترو-ضوئية و يمكن تمثيل هذه الحالة ب (0)، ثم يتم تجميع هذه الوحايد و الأصفار لتكوين ال**Bits** ثم ال **Bytes** . و أصعب جزء عملية القراءة من الأسطوانة هي في الحفاظ علي شعاع الليزر مركز علي منتصف مسار البيانات، وهي وظيفة منظومة التتبع . ويجب أن تقوم منظومة التتبع -أثناء تشغيل الاسطوانة- بتحريك منظومة الليزر للخارج، وهذا يؤدي إلي أن تكون سرعة مرور الأجزاء المرتفعة -المكونة لمسار البيانات- أمام شعاع الليزر أكبر، لذا يجب أن يقوم الموتور الذي يدير الأسطوانه بتقليل سرعته حتي تظل سرعة مرور الأجزاء المرتفعة مثبتة، وبالتالي يكون معدل قراءة البيانات من الأسطوانه مثبتاً . ملحوظة : لابد من التنبيه علي ضرورة الحفاظ علي الأسطوانات نفسها بشكل سليم باتباع الخطوات التالية :-

1- لا تترك الأسطوانة خارج الغلاف الخاص بها بعد استعمالها، لأن هذا الغلاف يحميها من الأتربة والغبار.

2- لاتضع أى شئ قد يعرض سطحها للخدش لأن سطحها رقيق وقابل للخدش.

سيف علي حسن الدار
+967/ 771323146-735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

3- عند إخراج الأسطوانة من غلافها أو من وحدة القرأة الخاصة بها قم بإمساكها من أطرافها الخارجية بأطراف أصابعك.

4- احرص على إدخال الأسطوانة داخل الوحدة بالوضع السليم فيكون السطح المكتوب عليه اسم الأسطوانة لأعلى.

5- عند تثبيت الأسطوانة داخل وحدة القراءة الخاصة بها تأكد من انها مستقرة جيدا فى مكانها الصحيح.

6- عندما ترغب فى كتابة عنوان على الأسطوانة لبيان محتوياتها فاكتبه على السطح المسموح بالكتابة عليه دون ان تضغط عليها بشدة مع تجنب الكتابة على الأسطوانة بقلم ذى سن حاد حتى لا يتسبب فى خدش سطحها بسهولة. تأثير الخدوش والأتربة علي القدرة علي القراءة السليمة للأسطوانات لأن الاتربة والخدوش تؤدي إلي تشتت شعاع الليزر القادم من القارئ، والمفترض ان ينعكس مرة أخري ليتم التعرف علي البيانات كما سبق شرحه وينتج عن تشتت شعاع الليزرعدم القدرة علي القراءة الصحيحة للبيانات مما يؤدي في النهاية الي فشل القراءة. ملحوظة : بعض الدراسات الحديثة أثبتت أن هناك نوعاً من البكترياً التي تتكاثر في ظروف الحرارة والرطوبة تتغذي علي الطبقة الداخلية للأسطوانات الليزرية خاصة إذا توافر لها ظروف النمو من حرارة ورطوبة فانها تتكاثر بسرعة كبيرة مما يؤدي إلي تلف الإسطوانة. فهل سيأتى اليوم الذي يتطلب فيه حفظ الاسطوانات في الثلاجة.أعطال شائعة والآن سوف نستعرض بعض الأعطال الشائعة في مشغل الاسطوانات وكيفية أصلاحها.

1- يقوم الجهاز بتشغيل بعض الأسطوانات والبعض الآخر لا .

2- الجهاز يقرأ الأسطوانات بصعوبة بالغة. العيب : إما أن يكون هناك بعض الأتربة العالقة علي عدسة الليزر أو أن هناك بعض الخدوش علي الاسطوانة نفسها. الصيانة : استعمل اسطوانات التنظيف لإزالة الأتربة عن العدسة ـ وقم بتنظيف الاسطوانات بواسطة قطعة من القطن الناعم.

3 ـ مشغل الأسطوانات لا يعمل رغم سماعي لصوت عمل الموتور وقيامي بتنظيف العدسة. العيب : وجود عطب بوحدة التتبع المسؤولة عن تحريك مجموعة الليزر وهنا إما ان تكون تالفة أو هناك عوالق تعوقها عن الحركة. الصيانة : قم بفك وحدة مشغل الأسطوانات متبعا تعليمات دليل التشغيل (لا تقم بذلك في حالة وجود ضمان) ثم قم بتنظيف الوحدة باستخدام تيار هواء ثم تأكد من انه لا يوجد ما يعيق عمل الوحدة من خلال إدارتها بإصبعك برفق .

4 ـ باب مشغل الأقراص لا يعمل . قم بفتحه يدويا باستخدام إبرة في المكان المخصص لذلك بالموجه الأمامى لمشغل الإسطوانات (يوجد ثقب صغير) ثم تاكد من عدم وجود إعاقة للباب وتأكد ان الموتور المخصص لحركة الباب يعمل جيدا.

5- كيف اقوم بتركيب مشغل اسطوانات جديد

1- تأكد من ان الجهاز مغلق ويفضل نزع كابل الكهرباء من الجهاز.

2- انزع الغطاء الخارجي للجهاز.

3- قم بادراج وحدة مشغل الاسطوانات بالمكان المخصص لذلك في الحاوية (Case) وثبتها جيدا بواسطة اربعة مسامير (غالبا ما تأتي مع المشغل).

4- قم بتوصيل كابل الطاقة (مع مراعاة التركيب الصحيح له بأن يكون طرف السلك الأحمر من الداخل.

5- قم بتركيب كابل البيانات مع مراعاة نقطتين الأولي : وضع *الجامبر* هل هو موضوع بوضعية جعل المشغل

هو الوحدة الاساسية علي كابل البيانات ام في وضعية الفرعية (Master/Slave) وغالبا ما يكون *الجامبر* في وضعية جعل المشغل فرعأي.. وذلك هام جدا في حالة ما إذا كنت سوف تركب المشغل مع الهارد أو أي وحدة أخري علي نفس الكابل. والثانية التأكد من أن الخط الأحمر بالكابل إلي الداخل

الموضوع السابع : معلومات عن فيروس جديد يتذكر لمساتك على لوحة المفاتيح

واصل فيروس الكمبيوتر الجديد "كورجو" الذي يصيب الاجهزة التي تعمل بنظامي "ويندوز 2000" و"أكس بي" ببساطة عند اتصالها بشبكة الانترنت انتشاره في أنحاء العالم أمس الجمعة حيث يقوم بإدخال جاسوس دقيق يستطيع تسجيل المفاتيح التى تضغط عليها في اللحظات السرية مثل طبع كلمات السر.
وظهر كورجو لاول مرة في 22 أيار/مايو وهو موزع الان في ست صيغ على الاقل. والعلاج هو في برنامج مجاني يطلق عليه اسم "كيه بي 835732" من موقع ميكروسوفت ولكن المحليين قالوا إن انتشار كورجو يفترض على ملايين مستخدمى أجهزة الكمبيوتر الشخصية أنهم لم يستخدموا العلاج بعد.
وقال كريستوفر فيشر وهو خبير ألماني في الفيروسات إنه لا توجد أية بوادر على أن كورجو أدى إلى زيادة كبيرة في حركة سير الانترنت.
وتستغل الدودة نفس المسار في النوافذ مثل فيروس ساسر وهو أكبر فيروس في العالم منذ نيسان/ابريل الماضي. ولا تصيب الدودة نظام ويندوز 98 أو أية أنظمة تشغيل أخرى. وقد أثارت شركات البرامج المقاومة للفيروسات تقييمها لتهديد كورجو بعدما وجدت أنه أصبح منتشرا.
وكان مراهق ألماني يدعى سفين جاشان قد اعترف بتصميمه فيروس ساسر مدعيا أنه جسم مضاد لقتل الفيروسات البغيضة الطليقة. وأوضحت شركة إف سيكيور وهي شركة فنلندية لمقاومة الفيروسات أن يكون فيروس كورجو نتاج عمل مجموعة قراصنة روسية تطلق على نفسها اسم "فريق المتطفلين".
وقال الصحفي توماس كريتشمان بمجلة بي سي الالمانية إن القرصان المبتكر لفيروس كورجو يحتاج للقيام بكم كبير من العمل التحليلي للتفرقة بين ضربات المفاتيح الخاصة بكلمات السر أو بطاقات الائتمان من لوحة المفاتيح الخاصة بالكمبيوتر. ولا يستطيع فيروس كورجو العثور على أو فك الشفرة المخزنة في القرص الصلب"الهارد درايف".
وقالت شركة سوفوس لبيع برامج مكافحة الفيروسات إن عدد الفيروسات المنطلقة على الانترنت في شهر أيار/مايو كسرت أكبر معدل سجل خلال العامين والنصف عام في الشهر الماضي.
وقد اكتشفت سوفوس على ما إجماليه 959 فيروسا جديدا على شبكة الانترنت في شهر أيار/مايو وهو أعلى رقم منذ كانون الاول/ديسمبر عام . 2001 وقالت إن منتجاتها تحمى ضد 90811 فيروسا مختلفا. وكان ساسر على رأس قائمة أخطر عشرة فيروسات في شهر أيار/مايو.
والجدير بالذكر أن الفيروس الجديد لا يدخل الكمبيوتر عبر البريد الالكتروني إنما عن طريق شبكة الانترنت ويتسبب في إعادة تشغيل الجهاز كل 60 ثانية كما يتسبب في بطء استخدام شبكة الانترنت.
وتصف شركة أمن المعلومات "سيمانتك" الفيروس الجديد بأن خطورته متوسطة وتعرض في موقعها على شبكة الانترنت أداة خاصة لتنظيفه من نظام التشغيل المصاب به. كما تعرض شركة "ميكافي" تحديث برمجيتها أيضا لانها تحتوي على ملفات حماية من الفيروس الجديد.

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146-735446181
saif201028@yahoo.com

الموضوع الثامن : كيف تواجه الحملة القذرة من اليهود على المواقع الإسلامية

لا يخفى عليكم الحرب الشرسة التى بدأت ضد المجموعات الإسلامية والعربية الموجوده حاليا
ولمواجهة هذه الحملة القذرة يجب علينا أن نوضح لجميع الأخوة
طريقة معرفة الرسالة التى تحتوى على
أولا ً:شرح للمشكلة
ثانيا ً: طريقة الأكتشاف قبل فتح الرسالة
ثالثا ً: طرق العلاج
======================
أولا ً:شرح للمشكلة
أن الذين يقومون ببعث هذه الرسائل يستخدمون بعض البرامج التى تتيح لهم أستخدام أسماء أيملات للأصدقاء و المعارف وهذا لكى يقع المسلم أو العربى فى الفخ ويفتح مرفقات الرسالة
بمعنى أكثر وضوحا:
أن من الممكن أن يرسل لك رسالة من شخص تعرفة وتكون هذه الرسالة تحمل الفيروس وهذا الصديق ليس هوا من قام ببعث هذه الرسالة ولكن من قام ببعث هذا الرسالة هوا هذة المجموعة
تعريف بالفيرس المستخدم:
اسم الفيروس هوا
W32.Sobig.F@mm
:Subject
Re: Details
Approved :Re
Re: Re: My details
!Re: Thank you
Re: That movie
screensaver Re: Wicked
Re: Your application
!Thank you
details Your
وعند فتح الرسالة سوف تجد مكتوب بداخلها :
:Body
the attached file for details See
.details Please see the attached file for
و المرفقات التى تحملها تكون :
:Attachment
your_document.pif
document_all.pif
thank_you.pif

aldare-1989@hotmail.Com
سيف علي حسن الدار
saif201028@yahoo.com
+967/ 771323146-735446181

your_details.pif
details.pif
document_9446.pif
application.pif
wicked_scr.scr
movie0045.pif

ثانياً : طريقة الأكتشاف قبل فتح الرسالة :

طريقة أكتشاف إذا كانت الرسالة المبعوثة تحمل فيرس و أنها ليست من صديقك الذى يملك الأيمال المستخدم لبعث الرسالة التى تحمل الفيروس

عندما تصل أليك رسالة تحمل أحد العناوين التالية قم بمسح الرسالة قبل فتحها:

Re: Details
Re: Approved
details Re: Re: My
!Re: Thank you
Re: That movie
Re: Wicked screensaver
Your application :Re
!Thank you
Your details

أذا أردة أن تفتح الرسالة ولكن بدون فتح المرفقات فأنك سوف تجد فى الرسالة مكتوب:See the : Body
.details Please see the attached file fo attached file for detail

أنا أفضل مسح الرسالة من قبل فتحها وهذا فى حالة وجود العنواين السابق ذكرها

ثالثا طرق العلاج:

1- يجب أن تقوم بتحيث مكافح الفيروسات الذى تملكة بأحدث نسخة من الأنترنت لأن لو لم تفعل هذا فأن فى هذه الحالة لم تستطيع أكتشاف الفيروس فى حالة الأصابة

2- يجب فحص الجهاز بالكامل بعد التحديث لكى تبحث هل اصيب جهازك بالفيروس أم لا

لأن فى حالة اصابتك بالفيروس سوف يستخدم الفيروس جهازك لبعث الرسائل التى تحمل الفيروس أكرر مرة أخرى يجب فحص الجهاز بالكامل لأن فى حالة أصابة جهازك سوف يستخدم الفيروس جهازك لبعث الفيروس

الرجاء اتخاد الحذر من المواقع التالية :

/http://www.answering-islam.org
/http://www.aboutislam.com
/http://www.thequran.com
/http://www.allahassurance.com

هذه المواقع على الأنترنت أصدرها اليهود الإسرائليون في محاولة لهم نشر معلومات زائفة عن الإسلام و القرآن و الحديث على الصعيد العالمي

الموضوع التاسع : إحذر من شاشات التوقف

هنالك أشخاص يقومون بإرسال شاشة توقف أو حافظة شاشة **SAVER SCREEN**
بها ضفادع باسم **Budweiser Frogs**
إذا قمت بتحميل هذه الشاشة في جهازك فسيقوم بتدمير القرص الصلب..
لا تقم بتحميلها تحت أي ظرف أو ضغط..
هذا يعتبر فيروس جديد.. والكثيرون لا يعرفون عنه شيء.
قم بإبلاغ أصدقائك بأسرع وقت ممكن
وهو فيروس خطير جداً ولا يوجد له مكافحة حاليا

الموضوع العاشر : تجربة في ملفات غريبه والإكتشاف بأنها فايروس

كن حذرا فهناك فايرس ظهر حديثا يقوم بمسح الدرايف c
فإذا وصلتك رسالة تحمل هذا العنوان
" Economic Slow Down in US"
فعليك حذف الرسالة فورا.. أما إذا فتحتها فسيقول لك
"restart now. do you want to continue Your system will"
وحتى إذا اخترت " لا" فسيقوم بإغلاق جهازك ولن تستطيع تشغيله مره أخرى
حاول إرسال هذا التحذير لأكبر عدد ممكن
ونشره على اكبر نطاق ممكن
حتى يتجنبوا أخطار هذا الفايرس
==============================
يوجد فيروس جديد أكتشف حديثا و عمله هو حذف جميع محتويات القرص الصلب .
إذا وصلك أيميل بعنوان **"Bush Osama Vs"**،
أحذفه فورا ، عند فتحه سوف يسألك السؤال التالي **the world will this war affect economy؟"**.
هل سوف تؤثر هذه الحرب على اقتصاد العالم ؟
و يوجد عدة أزره اذا ضغطت على أحدها سوف يتم ايقاف النظام عندك و لن تستطيع تشغيله مره أخرى .و قد سبب هذا الفيروس عدة مشاكل في أمريكا و الهند و بعض مناطق العالم .

إذا قام بإضافتك **meltdown@hotmail.com**
فلا تقبل الإضافة لأنه فيروس . أخبر كل الأشخاص الموجودون على قائمتك المسنجرية ،لأنه إذا قبل أحد منهم علىإضافته ستصاب أنت أيضا بالفايروس
هنالك فيروس جديد ينتشر بواسطة الإيميل عبارة عن رسالة فيها صورة حذاء أحمر يرقص مع موسيقى جميلة.

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

ويعرض عليكم من خلال الرسالة أكثر من 1000 أغنية للإستماع.
لا تقوموا بفتح أو إنزال هذه الرسالة أبداً للجهاز لأنها تحوي على فيروس قاتل بحيث خلال ساعتين يقوم بتخريب شامل للدسك الصلب **disk hard**
إسم الفيروس : **kleneu66** ولغاية كتابة هذه السطولر لا يوجد هناك مضاض لهاذا الفيروس ولا يمكن ايقافة حالياً

ما اكتبه هنا هو عبارة عن تجربة مريرة خضتها على مدى عطلة الاسبوع الفائته و احببت ان اشاركتكم اياها .....
احد زملائي اخبرني بانه يرى ملف اسمه **folder.htt** في كل مجلد يفتحه على الوندوز و لا يستطيع ان يفتحه ليرى ما في داخلة حيث تظهر له الرسالة المعروفة **access denied** اي ان الوصول الى هذا الملف ممنوع .....
اضافة للملف **folder.htt** فانه يجد ايضا ملف اسمه **desktop.ini** .... وهذا الملف يمكنه فتحه لكنه لا يجد فيه اكثر من 5 سطور ولا تشكل اي خطر من وجهه نظرة .... فكان سؤاله لي هل هذا فيروس او لا .... واذا كان فيروسا فهل يمكن ازالته و ما مدى الضرر الذي يلحقه بالجهاز ......
طبعا في البداية تذكرت اني قد رايت هذا الملف (**folder.htt**) في اكثر من جهاز على مقاهي انترنت ولكني لم اكترث حينها له ولم احاول حتى فتحه ..... لهذا وافقت ان اذهب مع صديقي الى غرفته لنكشف على الجهاز ونرى ما المشكلة ....
اول مجموعة ملاحظات كانت التالي ....
- الملفين **desktop.ini** و **folder.htt** ملفان مخفيان لكنهما يظهران لان صديقي اختار ان يظهر الملفات المخفية من قائمة **tools>>folderOptions** ..... ولولا انه اختار اظهار كافة الملفات منذ زمن لما لاحظ وجود الملفين (عندما تختار اظهار كافة الملفات تظهر الملفات المخفية اصلا بلون باهت مقارنه مع بقية الملفات)
- عند انشاء مجلد جديد فارغ في اي مكان على الجهاز ثم فتح المجلد نجد الملفان موجودان في داخله. ولكن عند انشاء مجلد جديد فارغ عن طريق الـ **DOS** ثم استعراض الملفات التي بداخلة من على الـ**DOS** ايضا لا نجد الملفين ولكن ما ان نستعرض المجلد نفسه من الوينْدوز ثم نعود و نستعرضه من الدوس حتى نجد انهما اصبحا موجودين في داخله.
- حجم الملف **folder.htt** حوالي 15 **KB** .
- الملف **folder.htt** لا يمكن فتحه ولا حذفه لا من الدوس و لا من الوندوز.
- الجهاز اصبح بطيئا بشكل ملحوظ عند فتح مجلد حتى ولو كان فارغا.
- عند ادخال قرص مرن في محرك الاقراص فانك بمجرد فتحه تجد الملفين موجودين في كل مجلد من مجلدات القرص المرن.
الآن بدأت فعليا اشك في انه فيروس،لكن جهاز صديقي عليه **Vairus McAfee Anti** ولم يعلن عن وجود فيروس في الجهاز ثم انني تذكرت شيئ مهم ....
اذكر منذ زمن انه يمكننا تخصيص مجلد ما من داخل الوندوز بحيث يظهر بشكل مختلف عن بقية المجلدات عندما نفتحه .... اقصد يكون له صورة معينة بدل الخلفية البيضاء العادية و يتغير لون و نوع الخط الذي تظهر به اسماء

الملفات...... عندما قرأت اسم الملف **folder.htt** ربطت بينه و بين هذه الميزة و اعتقدت ان الوندوز تنشئ هذا الملف و تحفظه في اي مجلد نقوم بتخصيصه اي انه ليس فيروسا وانما احد ملفات الوندوز المعروفة ....
وجدت ان استنتاجي المبدئي كان صحيحا عندما عدت الى جهازي السليم و بحثت عن ملف اسمه **folder.htt** ووجدته .... لكن المشكلة اني لم اجد سوى عدد قليل من الملفات وكلها لم يقل حجمها عن 20 **KB** .....
ففكرت بعمل تجربة .... جهازي يعمل عليه **Norton Anti Vairus 2003** ....
فقررت ان اجازف بادخال القرص المرن الذي جلبته من جهاز صديقي .... وبمجرد ان ادخلته ظهرت لي شاشه الـ

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146-735446181
saif201028@yahoo.com

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

Norton المشهورة التي تحذرك من وجود فيروس .... وكانت كما توقعت .... !!
الملف **folder.htt** مصاب بالفيروس **html.redlof.a** .... ولا يمكن اصلاحه ....
الآن تأكدت من صحه استنتاجي ...... فضغطت مباشرة على الرابط في الرسالة و الذي يأخذني الى موقع
symantec و يقدم شرحا وافيا عن الفيروس المذكور .... وهذه هي الصفحة
http://securityresponse.symantec.com....redlof.a.html
يعتبر هذا الفيروس من اخطر الانواع من ناحية الانتشار وهو يسمى **polymorphic** اي متعدد التشكل او عديد التشكل .... المهم انه من النوع الذي يقوم بانشاء نسخ من نفسه و ينتشر بهذه الطريقه .....وهذه بعض المعلومات عنه
هذا الفيروس عبارة عن **Visual Basic Script** ينسخ نفسه في مجلد النظام **system** او **system32** باسم **kernal.dll** او **kernal32.dll** ويصيب الملفات من نوع **html,htm,php,asp,jsp, vbs** ....
يقول موقع **symantec** انه يوجد 50 - 999 اصابة مسجلة لديهم مع اني اعتقد ان الرقم الحقيقي اكبر من هذا بكثير خصوصا واني قد رايت اجهزة اخرى مصابة بالفيروس ولم اعرف حينها انه فيروس .... اهم شيئ انه يقوم بعمل تعديلات معينه في الرجستري لكي يضمن ان يقوم النظام باعتبار اي مجلد هو مجلد مخصص و ينسخ الفيروس اليه .... على الاقل هذا ماعتقد انه يحصل .... ثم عندما تستعرض المجلد اذا كنت تستخدم اسلوب عرض المجلدات كصفحات ويب .... فانك لن تستطيع رؤية الملفات ولكنك سترى احرف غريبة تملا نافذه متصفح الوندوز ..... ولحسن الحظ ان صديقي لم يكن يستخدم هذا الاسلوب .... لكن المشكلة لا زالت قائمة ..... الفيروس " مبسط في جهاز الرجال و مسوى حفلات كل ليلة .... و سامري و بلوت و كل شي .... يعني ماخذ راحته على الآخر "
الآن ما الحل ...... كيف استطيع ازالته .... في البداية ..... ادركت انه لا يمكن حذف كل الملفات بكل بساطة .... ولكني بدأت احاول .....
ذهبت لموجة الدوس ثم نفذت المر التالي **folder.htt edit** طبعا امر **edit** يقوم بعرض محتويات الملف في محرر نصوص عادي على بيئة الدوس ..... لكن هذا لم يفلح فالملف لا يمكن الوصول اليه..... تماما نفس الرسالة التي تظهر في الويندوز ..... قمت بخدعه اخرى .... نفذت الامر التالي **edit** هذا الامر يفتح لك المحرر فارغا بحيث تستطيع الكتابة ثم حفظ الملف تماما كبرنامج النوت باد ..... وهنا استغليت الموقف و حفظت الملف "الفارغ" باسم **folder.htt** في نفس المجلد الذي يوجد فيه الملف **folder.htt** من قبل ..... ماذا تتوقعون انه حدث .....؟!
طبعا سالني المحرر " يوجد ملف اصلا باسم **folder.htt** هل تريد الحفظ عليه ؟ " فاجبت بنعم ... وحصل بالضبط ما توقعته ..... لقد تم محو الملف الاصلي ... وبشكل ادق ... اصبح الفيروس عبارة عن ملف فارغ باسم **folder.htt** ... وغير مخفي ... وطبعا حجمة **kb0** ..
فكرت بعدها .... هذه الطريقة لن تكون عملية ... فانا لن استطيع الدخول الى كل مجلدات القرص الصلب و تكرار نفس العملية في كل مرة .... اي اني لن استطيع ان افتح المحرر ثم احفظه بنفس الاسم في كل مجلد في القرص الصلب ثم و الاهم من هذا انها بمجرد ان تفتح ايا منها من الوندوز مرة اخرى ستجد ان الملف قد عاد على ماهو عليه .... و اصبح

الملف حجمه 15 **kb** مرة اخرى .... اذا ما العمل ....
يجب ان اوقف نشاط الفيروس التكاثري اي ان احاول منعه من نسخ نفسه في كل مجلد يتم فتحه من الوندوز .... و هنا عدت لموقع **symantec** .... فوجدت هذه التعليمات لازالة الفيروس يجب ان

1- تحدث تعريفات الفيروسات في برنامج النورتون
2- تعمل فحص شامل للملفات و احذف كل الملفات المصابة بالفيروس
3- اعكس العمليات التعديلات التي احدثها الفيروس في ملف الرجستري ...

سيف علي حسن الدار
+967/ 771323146-735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

الكلام اسهل من الفعل .... لاني في البداية اضطررت للبحث عن قرص تركيب برنامج النورتون وبعد ان ازلت McAfee الذي لم يكتشف حتى وجود الفيروس و ركبت Norton بعد جهد جهيد بدا يزعجني بشكل لا يطاق،حيث انني كلما فتحت اي مجلد اجد انه يظه لي رسائل التحذير التي لا تنتهي الى درجة اني فكرت في ان الغي تركيبة من على الجهاز .... لكني فكرت مرة اخرى .... بعد ان لاحظت ان الفيروس لم يعد ينتقل الى المجلدات الجديدة ....

فكل ما حاول ذلك يمنعه النورتون من تنفيذ الكود الخاص بالفيروس

و بالتالي لا يستطيع نسخ نفسه بعد الآن الى المجلدات الجديدة ..... لكن المشكلة ان الجزء الخاص بالفحص الشامل في النورتون و الذي يكتشف كل الملفات المصابة ثم يزيلها لا يعمل !! .... هكذا بكل بساطة لا يعمل !!

كلما ضغطت على الايقونة تظهر لي علامة الساعة الرملية ولكن البرنامج لا يعمل و عندما ابحث عنه في قائمة البرامج Alt+Ctrl+Del لا اجد اي عملية جارية لها علاقة بالنورتون .... هل يعقل ان الفيروس يمنع الجزء المتعلق بالفحص الشامل في نورتون من العمل ؟؟ .....!!! هذا ما لم اجد له جوابا ..... لكني حاولت بكل الطرق و شغلت النورتون عدة مرات .... و اعدت تشغيل الجهاز كذا مرة .... ولم تحل المشكلة النورتون لا يعمل ... الجزء الوحيد الذي يعمل هو الجزء المزعج .... التنبيهات التي لا تتوقف ولا تستطيع لا ازالة الملف ولا حتى احتوائة Quarantine .... ما العمل اذا ...

تركت الملفات المصابة الآن وشغلت الرجستري ...

run > regedit و تتبعت المسار التالي

1- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

ثم حذفت المدخل Kernel32 من الجزء الايمن ...

2- HKEY_CURRENT_USER\Identities\[Default Use ID]\Software\ Microsoft\Outlook Express\[Outlook Version].0\Mail

ثم حذفت القيم

Stationery Compose Use

Stationery @_@@_@@_@@_@

Wide Stationery @_@@_@@_@@_@

3- HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Outlook\Options\Mail

وحذفت EditorPreference

و اخيرا

4- تتبعت هذه المسارات

HKEY_CLASSES_ROOT\dllFile\Shell

HKEY_CLASSES_ROOT\dllFile\ShellEx

HKEY_CLASSES_ROOT\dllFile\ScriptEngine

HKEY_CLASSES_ROOT\dllFile\ScriptHostEncode

و حذفتها كلها ....

الآن المفروض ان الفيروس لا يستطيع التحكم بالمجلدات و نسخ نفسه اليها ....

سيف علي حسن الدار
+967/ 771323146-735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

بقيت امامي العقبة الاخيرة .... وهي ازالة الملفات المصابة .... طبعا الفيروس يصيب الملفات من نوع **htm** و **html** و و و لكنني الآن سارکز على الملفات المسماه **folder.htt** وهي التي تحمل الفيروس بشكل صريح خصوصا و اني لا استطيع ان اعرف اي الملفات الاخرى تحمل الفيروس بدون ان استخدم برنامج النورتون ..... لكن المشكلة ان المساعدة الواردة في موقع **symantec** تنتهي عند هذا الحد ... فهي تتطلب استخدام النورتون ..... و النورتون لا يعمل .... و المشكلة لا استطيع الاتصال بالانترنت حاليا .. ماذا افعل ؟

الحل يجب ان يأتي من الدوس ....

عدت مرة اخرى لموجه الدوس ....

وحاولت استخدام امر **del** مرة اخرى ...

لم ينجح .... استخدمت امر جديدا اسمه **erase** يقوم بنفس العمل .... ولم ينجح هو الآخر ...

ثم اهديت الى فكرة مجنونة ..... لمذا لا ازيل خاصية الاخفاء من الملف ثم احاول حذفه ..... و جربت

attrib folder.htt -h

فنجح الامر ....

ونفذت بعدها امر

attrib *.*

لاجد ان الملف **folder** تحول الى **R** و **A** اي انه اصبح ملف للقرائه و الحفظ ....

اها ... هل يمكن ان اقرا الملف الآن بواسطة محرر الدوس ..... كنت متشوقا لاعرف كيف كتب الفيروس .... لكن يبدو اني كنت ساذجا .... فلم اتمكن من قرائته حتى ببرنامج **hex editor** ...

لكنه الآن ليس مخفيا .....

اذا لمذا لا احاول ان احذفة مرة اخرى ...

del folder.htt

وكانت المفاجأة لقد تم حذف الملف!!

لم اصدق ما رأيت ....

عندها عملت **file patch** وهو ملف تنفيذي يحتوى سلسلة من اوامر الدوس التي تنفذ تباعا بدون ان يحتاج المستخدم لكتابتها كل مرة

وكتبت فيه الاوامر التاليه

folder.htt -h /s attrib

attrib desktop.ini -h /s

del folder.htt /s

desktop.ini /s del

طبعا الحرف **s** يعني ان يبحث في كل المجلدات الموجودة في السواقة و المجلدات التي داخل كل مجلد .....

طبعا بعد ان نفذت الملف .... الذي اسميته **folderhttFixer.bat** .... استغرق وقتا طويلا قبل ان يعلن لي وبكل زهو انه ازال كل ملفات الفيروس ولكن مهلا بقيت عدد من المفات من الانواع **htm** و **html** و **php** و غيرها .... ما العمل الآن ؟؟؟

عدت الى النورتون و بمجرد ان ضغطت على ايقونه الفحص الشامل ..... اشتغل البرنامج! و قام بفحص شامل و وجد حوالي 200 ملف من الانواع المذكورة ... وطبعا طلبت منه حذفها جميعا ....

واما الـ **file patch** الذي عملته .... فقد وجدت مفيدا مع الاقراص المرنه بمجرد ان انسخه الى احدها و انفذه

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

يمسح كل ملفات الفيروس و تعود الاقراص نضيفة مرة اخرى بدون الحاجة الى عمل فورمات و ضياع الملفات الاخرى المفيدة عليها

الموضوع الحادي عشر : سمعتم عن التروجان ؟ ما هو ؟ هنا الإجابة

ما هو التروجان ؟؟

تعريف:

التروجان هو برنامج تجسس و له أسماء أخرى مثل مخدم (Server) أو اللاصق (Patch) أو الجاسوس (Spy) لكن مبدعين هذا النوع من الملفات يفضلون الأسماء الرنانة و اسم تروجان هو نسبة إلى حصان طروادة. لكن مع اختلاف المسميات فهو برنامج تجسسي يجعل من حاسبك مخدم لحاسب الجاسوس، أي يتمكن الجاسوس (و هو الشخص الذي بعث إليك هذا التروجان) من التحكم بجهازك و كأنه أنت، لكن مع الأخذ بعين الاعتبار أن ذلك فقط في حال أنت متصل بالإنترنت أو الشبكة و ليس هذا فقط بل و عندما يعرف أنك على الإنترنت أما غير ذلك فهو لا حول له ولا قوة.

كيف يلج إلى التروجان إلى حاسبي:

1- عن طريق برامج المحادثة مثل Microsoft chat و ICQ و Mirc و MSN و Yahoo .. الخ.

فلا تستقبل أي ملف مهما يكن و خاصة التي يكون امتدادها exe و حالياً ظهرت برامج تقوم بتغير امتداد الصور إلى exe فبعض الهاكرز يستخدمها في الضحك على الضحايا و يقول لهم أنها صور مغير امتدادها إلى exeو لكنه قد يدس التروجان بداخلها أو قد تكون هي التروجان بحالها.

2- عن طريق البريد الالكتروني: لذا قم بحذف جميع الرسائل المجهولة و التي لا تعرف من هو مرسلها.

3- عن طريق تحميل برامج من مواقع مشبوهة: الحل : أن تفعل خاصية الحماية التلقائية لبرنامج Norton Antivirus و الذي هو أقوى برامج الحماية على الإطلاق لأنه يتعامل مع الفيروسات و برامج التجسس على حد سواء.

4- عن طريق المنتديات التي تفعّل خاصية html قد يأتي من هو حاقد على المنتدى و يزرع الكود في رد لموضوع أو في موضوع جديد.

الحل : بسيط جداً لأنه ليس من مسؤوليتك بل من مسؤولية مشرف الموقع.

5- عن طريق الماسنجر بأنواعها هناك برنامج جديد و لكني لا اعلم مدى مصداقية كاتبه و هو يقوم بعمل سرقة الملفات و الصور من جهاز الطرف الآخر إذا كان online و من دون إذنه و اسم البرنامج imesh .

الحل : لا تضيف إلا من تعرفهم و إذا صادفت أي شخص لا تعرفه و شكيت فيه فقم بعمل حظر ثم حذف، لكن إذا كان في جهازك تروجان و حظرته فسوف يدخل و أنت لا تعلم لأن الحظر لن يفيد ما دام الخادم في جهازك يستقبل أوامر العملاء، و أنا لي وقفة بسيطة حول هذا البرنامج قد يكون هذا البرنامج مثل أخواتها من التروجانات .. قد تسمح لمصمم البرنامج أن يتجسس عليك و أنت تحاول أن تتجسس على الآخرين عملاً بشعار افتراس المفترس و هذا هو حال كثير من برامج التجسس.

كيف أتخلص من التروجان إذا أصاب جهازي:

قبل كل شيء يجب أن تعرف أن الملف التجسسي إذا أصاب جهازك فإنه سوف يستوطن في واحد على الأقل من الأماكن التالية:

1- في الريجستري .

2- في الملف **Startup** .
3- في الملف **System.ini** .
4- في الملف **Win.ini** .
أما للتخلص منه فإليك الطريقة..
هناك طريقتين لحذف التروجان و هي مجربة على ويندوز 98 و هي إما بواسطة برامج الحماية و هذه هي الطريقة الأوتوماتيكية، أو الطريقة اليدوية عن طريق **DOS** و هي الأفضل و الأقوى من خلال التجارب مع **Trojans** إذا عملت بحث بواسطة برامج الحماية و صدف إنه في بعض الأحيان لا يمكن حذف التروجان بواسطة برامج الحماية لأن التروجان قد يحذف معه ملف مهم من ملفات النظام و في هذه الحالة تضطر إلى استخدام الطريقة الأخرى و هي الأفضل و الأسلم و هي كالتالي:
لنفرض أن التروجان اسمه **Server** تمكن من معرفته برنامج الحماية، أول خطوة و هي أن تتأكد هل هو يشتغل مع تشغيل الجهاز و ذلك بفعل التالي: اضغط على زر **start** اختر **run** اكتب:
msconfig
ثم اختر **Start UP** و من هناك ابحث عن اسم التروجان و غالباً ما يكون اسمه على الاسم الذي تم كشفه، ثم إذا وجدته أزل علامة الصح من أمامه ثم اعد تشغيل الجهاز. يمكنك مراجعة الطرق الاخرى بالضغط على هذه الوصلة
الخطوة الثانية و هي أن تحاول أن تجمع اكبر قدر من المعلومات عن التروجان الذي تم اكتشفاه حتى تتعرف عن أماكن اختبائه في الجهاز و عن تسجيل نفسه في الريجستري أو **Win.ini** أو **System.ini** أو جميعها معاً، و أفضل ثلاث مواقع يقدم لك الاستفسار الكامل عن أي تروجان
/http://www.dark-e.com/archive/trojans
/http://www.google.com
http://www.moosoft.com/tdbindex.php
الخطوة الثالثة بعد إعادة التشغيل ينبغي أن تكتب اسم التروجان كامل في ورقة خارجية ثم تذهب إلى الدوس عن طريق إعادة التشغيل و اضغط على **Ctrl** أو **F8** أو استخدام قرص الإقلاع اختار **Ms-Dos prompt** في حال كنت تستخدم **Win ME** أو عن طريق الدوس الخارجة عن نطاق الويندوز و هي من ابدأ ثم إيقاف التشغيل ثم اختر الرجوع إلى بيئة الدوس **MS-DOS MODE RESTART IN** و ذلك في حال أنك تستخدم **Win 98** ثم اتبع هذه الطريقة لكي تبحث عن التروجان و انتبه إلى المسافة بين الأمر **dir** و بين اسم التروجان و لا تنسى النجوم : *.*
dir server<C:/Windows *.* ثم إنتر و إذا وجدت أي ملف اسمه **server** و امتداده الأخير هو **exe** فهو مطلبك و عليك أن تحذفه بهذه الطريقة و انتبه إلى المسافة بين **deltree** و بين اسم التروجان ولا تنسى النجوم *.* : **Deltree server<C:/Windows** *.*
ثم إنتر ثم راح تسأل سؤال ضع علامة **Y** و قد يكون هناك أكثر من برنامج يحمل نفس الاسم و لكن الامتداد يختلف..
أهم شيء انك تبحث عن اسم التروجان **server** و الذي يكون امتداده **exe** هذه هي الطريقة اليدوية و الفعالة في حذف التروجان من الجهاز طبعاً تضع بدل من كلمة **server** الاسم الذي تم رصده من مكافحات التجسس.. ثم اعد تشغيل الجهاز.
ملاحظه مهمة جداً:
هناك أمر أخر للحذف و هو **Del** و لكني أفضل الأمر **Deltree** لأنه اشمل في الحذف و يقوم بحذف كل شيء مخفي من اثر التروجان و يتعقبه في كل الأدلة و ليس مثل الأمر **Del**و الآن نحن في الويندوز و بعدما تم حذف

التروجان و بقي أن نزيل بعض من آثاره من **win.ini** أو **system.ini** أو الريجستري. طبعاً بعدما تدخل إلى إحدى المواقع اللي فوق و بعدما تبحث عن اسم التروجان الذي تريده أن تعرفه عنه، و كان تروجانك هو **server** و حصلت على هذه المعلومات من المواقع السابقة و هي انه من فصيلة **Sub 7** و أهم شيء من المعلومات هذه من القسم **How To Remove** و عليك أن تتبع مسار التروجان في مكانه.. و بعد التمحيص عن التروجان وجدناه يسجل نفسه في الريجستري، اذهب إلى المفتاح التالي

HKET_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

و ابحث عن الأسماء التالية **EXPLO32, PATCH.EXE, RunDLL32r** ، **SERVER.EXEC** **WINDOWS\EXPL32.EXE, , Explorer32** في المفتاحين **Run** و **RunServices** و لاحظ على الملفات جيداً فإن لم يقابلها **Data** أو يظهر أمامها سهم صغير **à** فهو ملف تجسس إذ ليس له عنوان معيين في الويندوز، و عندما تجد احد تلك الملفات قم بحذفه، و بعدين تسوي إعادة تشغيل، و الآن عليك البحث في الملفين **Win.ini** و **System.ini** و اللذين تشغلهما من **Run** ثم اختر الملف **System.ini** و ابحث في قسم الـ **Boot** عن أي اسم غريب تحت هذا السطر **shell=Explorer.exe** ثم أزل منه الصح لكن تحقق من انه تروجان و هكذا. بعض التروجانات قد تحذف معها ملفات مهمة من الجهاز و في هذه الحالة يتطلب منك إرجاعها و طريقة الاسترجاع كالتالي:

في تشغيل **Run** اكتب **SFC** ثم إنتر ثم اختر الإعدادات **Settings** ثم في آخر شيء ضع علامة صح تفقد الملفات المحذوفة **Check for deleted files** ثم اختر موافق و بعدها اختر **Start** و اترك البرنامج يقوم بعمل فحص للملفات قد يكون هناك ملف محذوف و يتطلب رجوعه بواسطة **CD**.. طبعاً على حسب نوع النظام اللي عندك يعني إذا عندك نظام 98 لازم قرص 98 و هكذا إذا وجد ملف محذوف يطلب القرص و أكمل بعدها إجراءات استرجاعه

الموضوع الثاني عشر : أكبر موسوعة مصطلحات كمبيوترية

أصغر وحدات القياس

بت8 **Byte 8 Bit = 1 Character**

بايت 1024 **KB** 1024 **Byte = Kilobyte**

كيلو بايت 1024 **MB 1024 KB Mega Byte**

ميجابايت 1024 **GB 1024 MB Gaga Byte**

تيرابايت 1024 **TB 1024 GB Tetra Byte**

ملف تنفيذي **EXE Executable File**

ملف دفعي **BAT Batch File**

ملف أوامر **COM Command File**

ملف نصي **TXT Text File**

ملف نظام **SYS System File**

ملف صوتي **WAV Wave File**

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

MIDI Music Instrument Digital Interface Fileملف وسائط صوتي
MID Music Instrument Digital Fileملف وسائط صوتي
QT Quick Time Fileملف فيديو
BMP Bitmap Fileملف صورة
EMF Enhanced Meta Fileملف صورة
WMF Windows Meta Fileملف صورة
GIF Graphic Interchange Format Fileملف صورة
AVI Audio Video Interleave Fileملف فيديو
DOC Document Fileوثيقة وورد
MDB Microsoft Database Fileملف قواعد بيانات
MPEG Moving Pictures Experts Group Fileملف فيديو
PIC PC Paintملف صورة
TRC Audio Track Fileملف صوت قرص
JPEG Joint Photographic Experts Group Fileملف صورة
PNG Portable Network Graphics Fileملف صورة
TIFF Tagged Image File Format Fileملف صورة
PDF Portable Document Format Fileملف صورة
MP3 MPEG-Layer3audio Fileملف صورة

مصطلحات الحاسب.............2

WWW World Wide Webالشبكة العنكبوتية العالمية
.com Commercial Businessesموقع تجاري
.edu Higher Educationموقع للتعليم العالي
.org Organizationمواقع منظمات أو هيئات
.gov Governmentمواقع حكومية
.net Networkمواقع للشبكات
.mil Militaryمواقع عسكرية
HTTP Hypertext Transfer Protocolلغة نقل النص

HTML Hypertext Markup لغة إعداد @_@@_@@_@@_@@_@@_@@_@@_@
النص

DHTML Dynamic HTML الديناميكية HTML
FTP File Transfer Protocolلغة نقل الملفات
IP Address Internet Protocol Addressعنوان تعريف الإنترنت
ISP Internet Server Providerمقدمة خدمة الإنترنت
W3C World Wide Web Consortiumجمعية تحديد معايير لغة إنشاء الصفحات

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

الطرق المباشرة CGI Common Gateway Interface
بروتوكول من نقطة إلى نقطة P.P.P Point-to Point Protocol
بروتوكول تحكم النقل للإنترنت TCP/IP Transfer Control Protocol / Internet Protocol
غير متوفر حاليا SLIP Serial Line Interface Protocol
غير متوفر حاليا CSS1 Cascading Style Sheets 1
غير متوفر حاليا SSI Server Side Include
غير متوفر حاليا DOM Document Object Modal
خادم معلومات الإنترنت IIS Internet Information Server
خادم شبكة شخصي PWS Personal Web Server
غير متوفر حاليا IPP Internet Presence Provider
خادم أمن PGP Pretty Good Privacy
@_@@_@@_@@_@@_@@_@@_@@_@ غير متوفر حاليا XML Extensible Markup
صفحة الخادم النشطة ASP Active Server Page
المقبس أو البروتوكول ذو الطبقة الآمنة SSL Secure Socket Layer
التعامل الإلكتروني الأمن SET Secure Electronic Transaction
بروتوكول نقل البريد البسيط SMTP Simple Mail Transfer Protocol
غير متوفر حاليا NNTP Network News Transfer Protocol
الأسئلة المتكررة FAQ Frequently Asked Questions
الشبكة الرقمية للخدمات بسر عات 64 و 128 كيلو بايت ISDN Integrated Services Digital Network
بروتوكول خدمات النقاش NNTP Network News Transport Protocol
بروتوكول البريد الإلكتروني POP Post Office Protocol
البروتوكول التسلسلي للاتصال بإنترنت SLIP Serial Line Internet Protocol
اختصار وصلة إنترنت URL Uniform Resource Locator
خدمة المحادثة عبر الإنترنت IRC Internet Relay Chat

الموضوع الثالث عشر : طريقه تجعل سرعة اتصالك سريـعة بحيث تتصل بأكثر من سيرفر

وصف الطريقة :
هي إضافة قيم للريجستري بحيث يخليه يتصل بأكثر من سيرفر بدل سيرفر واحد ... يعني لما كنت تحمل الصور والصفحات والجافا وغيره وغيره بسيرفر واحد الحين حمـــل بأكثر من سيرفر ولاحظ سرعة التصفح
أولاً : إنسخ الكود التالي وضعه في برنامج المفكرة

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

REGEDIT4
]HKEY_USERS .
DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings"[Max Connections Per Server" =dword:00000020 " MaxConnectionsPer1_0Server="dword:00000020
]HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\ Internet Settings "[Max Connections Per Server" =dword:00000020 " MaxConnectionsPer1_0Server" =dword:00000020

ثانياً :إحفظ الملف في أي مكان على الجهاز بامتداد **reg** مثـــال **tasree3.reg**
واضغط "حفظ" ثم اذهب للملف المسمى " **tasree3.reg** " الذي تم حفظه من قبل واضغط عليه (افتحه) بيقولك هل تريد حفظ المعلومات للريجستري >>> موافق
ثالثاً : أعد تشغيل الجهاز
طريقة لتسريع الإنترنت في **Windows XP** بدون أي برنامج
هذه طريقة لتسريع الإنترنت بدون استخدام أي برنامج
الخطوات هي
1- قم بالدخول على الكمبيوتر كمشرف **Administrator**
2- من قائمة **Start** اضغط على **Run** واكتب **gpedit.msc**
3- في الجهة اليسرى اضغط على إشارة + التابعة لـ "**configuration Computer**"
4- اضغط على + التابعة لــ **Administrative templates**
5- اضغط على + التابعة لــ **Network**
6- اضغط على **QoS Packet Scheduler**
7- في القسم الأيمن اضغط مرتين على **limit reservable bandwidth**
8- في قائمة **Settings** اختر **Enable**
9- ستجد في نفس النافذة عنوان هو **Bandwidth limit %** غير النسبة إلى صفر من 20. اضغط **Apply** ثم أغلق النافذة
10- اذهب إلى **Network Connections**. إذا لم تعرف كيف تصل لها اتبع الخطوات **Start** ثم **Settings** ثم **Connections Network**.
اضغط على أيقونة الإتصال باليمين واختر **Properties**.
تأكد أن **Packet Scheduler Qos** مختارة
إن لم تكن مختارة أو مفعلة قم بتفعيلها

<u>الموضوع الرابع عشر : أوامر في الدوس تحتاج إليها مهم</u>
أوامر بالتاكيد سوف تحتاجها وأنت تعمل على جهازك الكمبيوتر .. فأحتفظ بهذه الصفحة .. لأنك سوف تعود إليها لاحقاً
ثم اكتب الامر الذي تريد من هذه الاوامر التي امامك**run** ثم تشغيل **star**لتنفيذ امر معين اذهب الى ابدا

سيف علي حسن الدار
+967/ 771323146-735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

هذا الامر لاظهار الاي بي لجهازك**Winipcfg**
اداة لتشخيص اخطاء النظام**Drwatson**
مهمته : أخذ لقطة عن النظام عند حدوث أي خطأ فيه.
.Drوتعرض هذا الأمر أخطاء البرنامج، وتعرّف البرنامج الذي أخطأ، وتقدم وصفاً مفصلاً لسبب الخطأ. وبإمكان في أغلب الأحيان تشخيص المسألة واقتراح سير الإجراءات. وعند اتصالك بالدعم الفني في **Watson** هو الأداة المستخدمة لتقييم المشكلة **.Dr. Watson** للحصول على المساعدة، فإن **Microsoft**
هذا الامر لادوات النظام وشاشة بدء التشغيل، و هدف هذا الأمرمساعدة تكوين النظام **Msconfi**
هذا الامر للوصول الى الرجستري لعمل بعض التعديلات التي تريدها **Regedi**
هذا الامر يقوم بتشغيل شاشة الدوس**Command**
هذا الامر لتنظيف الاقرص فقط حدد محرك الاقراص المراد تنظيفه ثم اضغط على موافق**.CLEANMGR.EXE**
هذا الامر لعمل تجزئة القرص الصلب .. عند استخدامه اضغط على اعدادات للاطلاع على الخيارات المتاحة**Defrag** او لتعديلها حسب رغبتك .
هذا الامر للتدقيق في الجهاز من ناحيتي الملفات والنظام بحثا عن الاخطاء واصلاحها انقر فوق محرك **ScanDisk** الأقراص الذي يحتوي على الملفات والمجلدات التي تريد التدقيق فيها.تحت نوع الاختبار، انقر فوق قياسي. ثم انقر فوق البدء.
مدقق تسجيل ويندوزلتفحص التسجيل**SCANREG**
وظيفته : يحتفظ نظامك دوماً بنسخة احتياطية عن تكوين التسجيل
(بما فيها معلومات عن حساب المستخدم، وروابط البروتوكول، وإعدادات البرامج، وتفضيلات المستخدم).
في كل مرة تعيد فيها تشغيل الكمبيوتر، يقوم مدقق التسجيل تلقائياً بتفحص التسجيل.
إذا لاحظ مدقق التسجيل وجود مشكلة، فهو يستبدل تلقائياً التسجيل بالنسخة الاحتياطية. إذا احتوى التسجيل على إدخال يشير إلى ملف لم يعد موجوداً (مثل ملف **.vxd**)، فلن يتم تصحيحه بواسطة مدقق التسجيل.
هذا الامر لتشغيل معالج الصيانة ومن مهامه**tuneup**
1 / تسريع البرامج المستخدمه بشكل متكرر
2/ تدقيق القرص المثبت لاستكشاف الاخطاء
3/ حذف الملفات الغير ضرورية من الجهاز
TUNEUP.EXEويمكن استخدام هذا الامر لنفس الغرض
تبحث أداة التحقق من التوقيع عن الملفات الموقعة وغير **microsoft** اداة التحقق من التوقيع لـ**SIGVERIF** . ويفيد التوقيع بأن **Microsoft**الموقعة على الكمبيوتر. الملف الموقع هو الملف الذي تم منحه توقيعاً رقمياً من الملف عبارة عن نسخة غير معدّلة من الملف الأصلي. ويمكنك بواسطة أداة التحقق من التوقيع القيام بما يلي:
عرض شهادات الملفات الموقعة للتأكد من عدم التلاعب بها.
البحث عن ملفات موقعة في موقع معيّن.
البحث عن ملفات غير موقعة في موقع معيّن
محرر تكوين النظام لاينصح بتغيير اي شيء فيها الا من قبل الخبراء او من لديهم معرفة تامه **SYSEDIT** بالتعديلات التي يريدون عملها على هذاالمحرر
يمكنك استخدام مدقق ملفات النظام للتحقق من تكامل ملفات نظام التشغيل، ولاستعادتها إذا كانت معطوبة، **SFC** ولاستخراج الملفات المضغوطة (مثل برامج التشغيل) من أقراص التثبيت.

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

لتثبيت **Windows Update** إلغاء تثبيت معالج التحديث وظيفته كالتالي ربما قد استخدمت **UPWIZUN** إصدار محدّث من أداة تصحيح، أو برنامج تشغيل، أو أداة نظام. إذا قررت فيما بعد إلغاء تثبيت الإصدار الجديد، ولم تتمكن من إعادة تأسيس الاتصال بإنترنت، استخدم إلغاء تثبيت معالج التحديث للعودة إلى الإصدار السابق.

اداة تشغيل عامل برنامج تشغيل التخطي التلقائي**asd.exe**

عن **Windows**) حالات الفشل التي تسببت في توقف **ASD**وظيفته : يعرّف برنامج تشغيل التخطي التلقائي (الاستجابة في عمليات بدء التشغيل السابقة ويضع عليها علامات بحيث يتم تجاوزها في عمليات بدء التشغيل اللاحقة. لتمكين أي جهاز تم تعطيله **ASD** كافة الأجهزة أو العمليات التي فشل بدء تشغيلها. ويمكنك استخدام **ASD**يذكر استخدام الجهاز في محاولة بدء التشغيل التالية. وفي حال الفشل، **Windows**، وسيحاول **ASD**سابقاً بواسطة تشغيل العملية سامحاً لك ببدء **ASD**يتوقف الكمبيوترعن الاستجابة. وعند إعادة تشغيل الكمبيوتر مرة أخرى، يمنع تشغيل الكمبيوتر

<u>الموضوع الخامس عشر : أهم الأسئله الشائعة وإجابتها</u>

مــاالـفـرق بـيـن أسـطـوانـات **CD-R** و **CD-RW** ؟

CD-R هى أختصار "**CD Recordable**" وهى تمكنك من الكتابة مرة واحدة فقط وليس لديك القدرة على مسح البيانات.

CD-RW وهى أختصار "**CD ReWritable**" وتتمكن من كتابة ومسح البيانات فيها عدة مرات .

لـمـاذا يـخـتـلف لـون الأسـطـوانـة مـن الأسـفل ؟

هذا يرجع لأن كل شركة لها تقنية فى تصنيع الأسطوانة من حيث أختلاف طبقات الصبغة الكيميائية .

ولكن لا يوجدالى الأن تقنية أفضل من الأخرى

مـاذا تـعـنـى سـرعـة الـرايـتـر **x4x32x6** ؟

ان الـ **x** ينقل 150 كيلو بايت فى الثانية

- أكبر رقم هو سرعة القراءة .
- الرقم الوسط هو سرعة الكتابة .
- أصغر رقم هو سرعة أعادة الكتابة .

واحيانا يتساوى رقم الكتابة "الحرق " مع رقم اعادة الكتابة .

مـاذا تـعـنـى هـذه الـصـيـغ **ISO9660** و **Joliet** و....؟ ومـا هـو الـفـرق بـيـنـهـم ؟

1) **CD-DA** أو **Red Book** وهذه الصيغة خاصة بأسطوانات الموسيقى "**MP3 , WAV**" .

2) **ISO9660** وهو أختصار **International Standards Organization**

ان هذه التقنية مقيدة فمثلا..

أقصى حد لأسم الملف هو "8 حروف " واقصى حد لمستوى الملفات هو 8 فقط

3) **Joliet** وهى من ابتكار مايكروسوفت ، ومن مزاياها

- اسم الملف من الممكن ان يصل الى 64 حرف .
- مدعمة لنظام ماك و لينوكس.

4) **HFS** وهى مخصصة لنظام الماكنتوش .

5) **ISO 9660** تستخدم بشكل خاص لأنظمة اليونكس واللينوكس .

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

6) **Level 2 ISO** وهى النسخة المطورة من **ISO 9660** " تسمح ان يكون اسم الملف لـ 31 حرف " ولكن هذه الصيغة لا تتوافق جيدا مع انظمة التشغيل .

مـاذا يـعنـى **multisession** ومـتـى يـجـب اسـتـخـدامـها ؟

وهى تقنية لأضافة البيانات على الأسطوانة

انت تستخدم **multisession** عندما تكتب بيانات" 100 ميجا " على الأسطوانة وتريد ان تضيف بيانات مرة أخرى .

اما فى حالة عدم أستخدام **multisession** فهنا تكتب على الأسطوانة مرة واحدة فقط مهما كان حجم البيانات التى بها .

هل يـمـكـننى ان اعـلـم مـدة الـقـراءة والـكـتـابة لـلأسـطـوانة بالكـامـل ؟

نعم عن طريق قسمة 74 على السرعة

فان كان سرعة الكتابة **x8** اذن كتابة "حرق" الأسطوانة كلها يأخذ" 8/74 " حوالى 10 دقائق

<u>الموضوع السادس عشر : معلومات غريبه عن البروكسي (proxy)</u>

المفوض او الوكيل (**proxy**)

بروكسي كلمه انجليزيه تعني الوكيل وتقوم مزودات بروكسي بدور الوسيط بين المشتركين لدى احدى شركات تقديم خدمه انترنت وبين المواقع الموجوده على الشبكه العالميه او بدور الوكيل عن هؤلاء المشتركيين في طلب المعلومات من تلك المواقع ونستطيع ان نتخيل مزودات البروكسي كذاكرات كاش كبيره الحجم مهمتها تسريع الحصول على المعلومات من واقع ويب واداء بعض الوضائف الأخرى

كيف تتم عملية الأتصال بينك وبين البروكسي

اذا اردت مشاهد صفحة ويب فان برنا مج التصفح لديك سينشئ اتصالا ً بينه وبين موقع الشركه ويطلب قرائة وثيقة (**HTML**) وينقلها الى جهازك ولنفترض ان شخصا ً اخر اراد زياره نفس الموقع في نفس الوقت فان العمليه السابقه ستتكرر مره اخرى وهاذا مايؤدي الى اشغال خطوط المزود الذي تتصل عبره بشبكه انترنت لطلب المعلومات ذاتها في نفس الوقت او خلال فترات زمنيه متقاربه خصوصا ً عندما يتعلق الأمر بزياره موقع مشهور بكثرة الزوار اما اذا جهزت برنامج التصفح لديك لاستخدام مزود بروكسي فانه سيتصل بهاذا المزود ويطلب منه احضار الصفحه المطلوبه وهنا يبحث مزود البروكسي عن الصفحه المطلوبه في قاعدة بياناته ليرى ان كان هناك نسخه منها اذا وجد البروكسي الصفحه ضمن قاعدة بياناته فانة يرسلها اليك مباشره اما ان لم تكن موجوده لديه فانه سيطلبها من موقع ويب ويرسلها اليك ويخزن نسخه منها في قاعدة بياناته في الوقت نفسه وعندما يطلب مشترك اخر(يستخدم البروكسي نفسه) الصفحه فان البروكسي سيرسلها اليه من قاعدة بياناته مباشره وبسرعه كبيره

<u>الموضوع السابع عشر : أعـرف كـل شـيء عن الـذاكـرة والأسـئـلة حـولـها</u>

أكثر من عشرين سؤال من الأسئلة الهامة والشائعة عن الذاكرة **RAM** وإجابتها بأسلوب مبسط دون التوغل في التفاصيل مع ملاحظة ان الأسئلة متدرجة حسب درجة الصعوبة ، لو كان لديك أي سؤال خاص بالذاكرة فلا تتردد في طرحه في ساحة النقاش " مناقشة المقال "

ما هى الذاكرة "**RAM** " و ما هى وظيفتها الأساسية ؟

ان الذاكرة والتى تعنى **RAM** اختصار لـ **Random Access Memory** والتي تعنى باللغة العربية ذاكرة

الوصول العشوائي وتتمثل وظيفتها الأساسية انها وسيلة حفظ مؤقتة للملفات والبرامج التي يتم استخدامها أثناء تشغيل الكومبيوتر وبمجرد غلق الجهاز يتم تلقائيا مسح جميع البيانات المخزنة على الذاكرة "RAM" ..

ما هي الفوائد من تحديث الذاكرة ؟

تحديث الذاكرة يعتبر اسهل وارخص طريقة لتحديث النظام ككل

إن تحديث الذاكرة مناسب للأشخاص الذين يتعاملون مع الملفات الضخمة ، ومع الذين يقوموا بتشغيل عدة برامج في نفس الوقت ، ومع الذين يتعاملوا مع البرامج والألعاب D3 ، وأخيرا مع الذين يتعاملون مع برامج الفيديو.

ما هو الوقت المناسب لتحديث الذاكرة ؟

- إذا كنت تلاحظ بطئ مؤشر الفأرة "الحركة الخاصة بالمؤشر تقطع "

- وفى حالة علو صوت القرص الصلب

- وفى حالة بطئ الجهاز بصفة عامه لا تتوقعها

كل هذه علامات لتحديث الذاكرة

وسبب هذا لأن في حالة امتلاء الذاكرة فان النظام يقوم بنقل البيانات إلي القرص الصلب بدلا من الذاكرة " Swapping"

ومادام القرص الصلب سرعته أقل بكثير جدا من الذاكرة إذاً ستكون النتيجة هي بطئ النظام

يكفى أن تعرف إن الذاكرة أسرع من القرص الصلب بحوالي 100 مرة.

هل إضافة المزيد من الذاكرة بأحجام مختلفة و بسرعة مختلفة يؤثر على سرعة الجهاز بالسلب ؟

لا فأنت يمكنك إضافة ذاكرة بأحجام مختلفة وسيكون سرعتها هي مجموع هذه الرامات .

هل شراء قرص صلب ذات سعة كبيرة يسرع من أداء الجهاز ؟

أولا إن الفرق بين القرص الصلب " Hard Disk " والذاكرة هو أن القرص الصلب يعتبر مخزن دائم للبيانات والملفات التي تحتفظ بها وتظل موجودة حتى لو طفئت الجهاز

أما الذاكرة فيخزن بها فقط البرامج والتطبيقات المشغلة فعلا وبمجرد إطفاء الجهاز تمسح جميع هذه البيانات

ولهذا فان زيادة سعة القرص الصلب لا يؤثر على سرعة الجهاز ولكن يمكنك فقط من تخزين المزيد من الملفات والبيانات .

هل تحديث الذاكرة يؤثر على سرعة المعالج ؟

بصفة عامة إن تحديث الذاكرة لا يؤثر على سرعة المعالج ، فالذاكرة والمعالج يعتبرا وحدتان يكملان بعضهما البعض .

ما هو حجم الذاكرة المناسب ؟

يعتبر 128 مناسب جدا الأن "وخاصة أن الأسعار فى انخفاض مستمر " واذا كنت من هواة الرسوميات وتريد أداء افضل فعليك بـ 256

هل عندما أضيف المزيد من الذاكرة يؤثر على الذاكرة الافتراضية ؟

لا انهما مختلفين تمام فالذاكرة الإلكترونية هي جزء يحجز على القرص الصلب ولكنها أبطأ بكثير من الذاكرة "القرص الصلب تقريبا أبطأ 100 مرة من الذاكرة " .

ومن الممكن أن تلاحظ في حالة إضافة المزيد من الذاكرة يؤدى لنقص حجم الذاكرة الافتراضية .

هل أضافه المزيد من الذاكرة يسرع التصفح بالإنترنت ؟

إن سرعة التصفح على الإنترنت تعتمد على الكثير من العوامل مثل " سرعة الاتصال ، مزود الخدمة ، الموقع الذي تقوم بزيارته

وبالنسبة لأضافه ذاكرة فأنك حتما ستلاحظ الفرق إذا كنت تستخدم عده برامج وتطبيقات أثناء تصفحك الإنترنت .

لماذا أصبح الكومبيوتر بطئ بعد إضافة المزيد من الذاكرة ؟

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

إن الشيء الطبيعي عند إضافة المزيد من الذاكرة يؤدى لزيادة سرعة الكومبيوتر ، ولكن نادرا من أن يحدث العكس وهو بطئ الجهاز وسبب هذا يكون إن الجهاز لا يوجد به كاش كافي لإضافة المزيد من الذاكرة ، والحل الوحيد هنا هو تحديث النظام أو اللوحة الأم .

إني املك ذاكرة 32 وأريد إضافة 64 في الشق الثاني فهل يؤثر هذا على الأداء ؟

باختصار يمكنك من إضافة سرعات مختلفة مع بعض في نفس الوقت

ولكن أهم شئ هو أن تضع الأكبر حجما 64 في الشق الأول والأقل في الشق الثاني .

ما هي الطريقة لمعرفة إذا كان يوجد شق فارغ لإضافة المزيد من الذاكرة ؟

لا توجد طريقة الا بفتح الهيكل "case "

لماذا لم تزيد مصادر نظام الويندوز **System Resources** عندما أضفت ذاكرة إضافية ؟

يعتقد الكثير من الناس أن مصادر النظام تزيد في حالة تحديث الذاكرة وهذا اعتقاد خاطئ وهذا لأن مصادر النظام ليس لها علاقة بالذاكرة ولكنه له علاقة بنظام التشغيل ويتأثر أيضا بالبرامج التي يتم تشغيلها

إذا كانت اللوحة الأم لدى تدعم 256 رام وهذا كحد أقصى لها ، وأنا أريد أن أضع 512 رام ، فماذا ستكون نتيجة هذا ؟

نحن لا نشجع على الأقدام على مثل هذه الخطوة ، ولكن إذا حدث فإما الجهاز سيتعامل مع الرامات المحددة له كحد أقصي " في مثالنا 256 " والذاكرة التي تزيد عن هذا لن يتعامل معها

وفى الغالب سيتعرف الجهاز على الذاكرة الإضافية ولكن سيؤثر هذا بالسلب على الكاشات والتي تكون نتيجتها عدم قيام الجهاز أو البطيء الشديد

هل أشترى رامات **PC100** ام **PC133** ؟

لو كان الكومبيوتر يدعم 133 **MHz** فأنت تحتاج ذاكرة **PC133** أما إذا كان الكومبيوتر لا يدعم إلا **PC100** فيمكنك استخدام أي نوع منهما ولكن السرعة ستكون 100 ، بشكل عام إذا كنت تنوى تحديث الكومبيوتر في المستقبل مع الاستمرار مع النوع **SDRAM** فأشترى ذاكرة من النوع **PC133**

هل من الممكن ان أستخدم رامات **PC100** مع **PC133** ؟

بشكل عام يمكنك من عمل هذا ، والذاكرة الأسرع ستعمل بسرعة الذاكرة الأقل سرعة "في هذه الحالة **PC100** " ، ولكن يوجد بعض الأنظمة لا تدعم هذا فعليك التأكد أولا .

ماذا تعنى هذه الأرقام **PC100, PC133, PC16**00، **PC2100** ؟

أولا بالنسبة للذاكرة **SDRAM** فان الأرقام التي تأتى بعد كلمة **PC** فإنها تشير لسرعة الناقل الأمامي فالنوع **PC133** مثلا يشير إلى إن سرعة الناقل الأمامي هي 133 وهذا النوع من الذاكرة يستخدم في أنظمة من النوع **Pentium II, Pentium III, AMD K6-III, AMD Athlon , AMD Duron**

إما بخصوص الذاكرة من النوع **DDR** فالأرقام التي تأتي بعد كلمة **PC** فإنها تشير إلى سرعة نقل البيانات في الثانية فالنوع **PC2100** مثلا يشير إلى إنه يتم نقل البيانات بسرعة 2.1**GB** في الثانية تقريبا وهذا النوع من الذاكرة يستخدم في أنظمة من النوع **XP" MP & AMD Athlon** " وبعض من أنظمة **Pentium III**

بعد أن أضفت المزيد من الذاكرة ظهرت لي هذه الرسالة " **Invalid system disk Replace disk and press any key**" والجهاز لا يتمكن من القيام ؟ فما العمل

من اكثر الأسباب الشائعة لحدوث هذا هو أثناء وضع الذاكرة تم تحريك الكابلات "مثل كابل القرص الصلب " ولهذا فأول شئ عليك عمله هو أن تتأكد من أن جميع الكابلات موضوعة بشكل صحيح وتأكد من سماع صوت القرص الصلب عند القيام .

ومن الممكن ايضا وجود ديسك فى الفلوبى فتأكد من عدم وجود اى ديسكات .

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

ولكن إضافة الذاكرة لا تؤدى إلى هذه النتيجة وإذا كانت المشكلة مازلت مستمرة فعليك بالرجوع للشركة المصنعة .
لدي ذاكرة أكثر من 512 ولكن الويندوز يعطيني رسالة " **out of memory** " .. فما سبب هذا ؟
سبب هذا هو انه لا يوجد في **Me Windows 95, 98** حجم كاشات مناسب لضبط أداء الذاكرة .. عليك بالرجوع لموقع مايكروسوفت لمعرفة الحل
http://support.microsoft.com/support.../Q253/9/12.asp
ما هي الذاكرة **RDRAM** ؟
RDRAM نوع من الذاكرة بالسرعة العالية لنقل البيانات وبكفاءتها وهى لا تختلف كثيرا عن الذاكرة من النوع **SDRAM** فلا يوجد اختلاف في طريقة إرسال البيانات أو استقبالها ولكن الذي يختلف هي طريقة التعامل هذه الذاكرة مع باقي أجزاء النظام
وهذا النوع يتوافر في ثلاثة سرعات **PC600, PC700 , PC800** والـ **PC1066** سيظهر قريبا
ومن مميزاتها أن الشريحة تنقسم لعدة أقسام **Device** وكل قسم فيها يكون في حالة من هذه الحالات أما أن يكون مطفئة أو في حاله رقاد أو الاستعداد أو إنها تعمل بالفعل في قراءة وكتابة بيانات وميزتها أيضا أن الشريحة تحتوى على عدد قليل من الـ **Pins** ولكن يعاب على هذا النوع ارتفاع سعره
ونتيجة لطبيعة عمل هذا النوع من الذاكرة فانه يجب أن تملئ جميع الشقوق بشرائح من الذاكرة أو بشرائح مكملة للدورة هذا في رقائق **i840 & i850**، أما بالنسبة للـ **Chipset** من النوع **i820** فيمكن أن توضع بعدد فردى
هل **DDR** أسرع من الـ **SDRAM** ؟
ان سرعة نقل البيانات **DDR** أسرع من الـ **SDRAM** ولكن ليست سرعة مضاعفة ولكنها بشكل عام أفضل من الـ **SDRAM** من حيث الكفاءة والأداء .
هل أتمكن من دمج ذاكرة من النوع **parity** مع ذاكرة من نوع **non-parity** ؟
لا تتمكن من فعل هذا وهذا بسبب أن الذاكرة من نوع **parity** بها نوع رقاقة خاص بها وظيفته التأكد من صحة البيانات وهل الذاكرة تقرأ وتسجل البيانات بصورة صحيحة أم لا
هو الفرق بين الذاكرة من نوع **ECC** والذاكرة من نوع **non-parity** ؟ وهل يوجد فرق في الأداء بينهم ؟ وأي النوعين مناسب لي ....
أولا إذا كان لديك ذاكرة ولا تعلم من أي النوعين هي فعليك بمعرفة عدد الرقاقة السوداء الموجودة على الذاكرة ، إذا كان عددهم يقبل القسمة على 3 أو 5 فنوع الذاكرة هو **ECC**
إذا كنت مقبل على شراء جهاز جديد ولا تعلم أي النوعين مناسب لك فعليك بمعرفة طبيعة استخدام الجهاز ، إذا كان سيستخدم كخادم **server** فعليك هنا باختيار النوع **ECC**
أما إذا كان سيستخدم للاستخدام المنزلي أو في مكتب فتعتبر الذاكرة من نوع **Non-parity** هي المناسبة
أما بالنسبة للأداء فيجب أولا أن نعرف معنى الذاكرة من النوع **ECC** والفرق بينها وبين الذاكرة من النوع **Non-parity**
إن **ECC** هي اختصار لكلمة "**Correcting Code Error**" وهذا يعنى في حالة وجود أخطاء في البيانات يتم تصحيح هذه البيانات دون أن يشعر المستخدم بذلك ولهذا فاستخدام هذا النوع من الذاكرة يزيد من أداء الجهاز نحو 2 % من ناحية صحة البيانات وكفاءتها
أما الذاكرة من النوع **Non-parity** فلا توجد بها خاصية تصحيح البيانات ولهذا ستلاحظ أنها أسرع من النوع **ECC**
هل من الممكن أن استخدم ذاكرة من النوع **ECC** مع لوحة أم لا تدعم هذه الخاصية ؟

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

إن هذا يعتمد على طبيعة برنامج الـ **Bios** الخاص باللوحة الأم فيوجد أنواع منه تقبل هذا ولكن يتعامل معه على انه **Non -ECC** وأنواع أخرى لا تقبل هذا

ما الفرق بين الذاكرة من النوع **buffered** والذاكرة من النوع **registered** ؟

بأختصار ان الذاكرة من النوع **buffered** تقوم بحجز مساحة مؤقتة " **Buffer** " في حالة التحميل الزائد للذاكرة

اما الذاكرة من النوع **registered** فهى تقوم بتأخير البيانات ليتم ارسالها فى دورة واحدة بدلا من ارسال كلا على حده وهذين النوعين من الذاكرة يستخدموا لأجهزة الخادمات **Server**

الموضوع الثامن عشر : تصفح الإنترنت بدون ماوس

هذه بعض الاختصارات للاكسبلورر التي جمعتها من بعض الكتب والمواقع

استكشاف صفحات ويب

اضغط هنا للقيام بـ

F11 التبديل بين ملء الشاشة والعرض المنتظم لإطار المستعرض

TAB التحريك للأمام عبر العناصر على صفحة ويب، شريط العناوين، وشريط **Links**

SHIFT+TAB التحريك للوراء عبر العناصر على صفحة ويب، شريط العناوين، وشريط **Links**

ALT+RIGHT ARROW الإنتقال إلى الصفحة التالية

ALT+LEFT ARROW الإنتقال إلى الصفحة السابقة

SHIFT+F10 عرض قائمة اختصارات للارتباط

CTRL+TAB تحريك إلى الأمام بين الإطارات

SHIFT+CTRL+TAB تحريك إلى الوراء بين الإطارات

UP ARROW تمرير نحو بداية المستند

DOWN ARROW تمرير نحو نهاية المستند

PAGE UP تمرير نحو بداية مستند في زيادات أكبر

DOWN PAGE تمرير نحو نهاية مستند في زيادات أكبر

HOME تحريك إلى بداية المستند

END تحريك إلى نهاية المستند

CTRL+F العثور في هذه الصفحة

F5 or CTRL+R تحديث صفحة ويب الحالية فقط إذا كان الطابع الزمني لإصدار ويب مختلفاً عن الإصدار المحلي المخزن لديك

CTRL+F5 تحديث صفحة ويب الحالية، حتى لو كان الطابع الزمني لإصدار ويب مماثلاً للإصدار المحلي المخزن لديك

ESC إيقاف تحميل الصفحة

CTRL+L or CTRL+O الانتقال إلى موقع جديد

CTRL+N فتح إطار جديد

CTRL+W إغلاق الإطار الحالي

CTRL+S حفظ الصفحة الحالية
CTRL+P طباعة الصفحة الحالية أو الإطار النشط
ENTER تنشيط ارتباط محدد
CTRL+E فتح البحث في شريط **Explorer**
CTRL+I فتح المفضلة في شريط **Explorer**
CTRL+H فتح المحفوظات في شريط **Explorer**
CTRL+click في شريط المحفوظات أو شريط المفضلة، فتح مجلدات متعددة
استخدام شريط العناوين اضغط هنا للقيام بـ
ALT+D تحريك مؤشر الماوس إلى شريط العناوين **F4** عرض محفوظات شريط العناوين
CTRL+LEFT ARROW عندما تكون في شريط العناوين، قم بتحريك رأس المؤشر الأيسر إلى الفاصل المنطقي التالي(. أو /) **CTRL+RIGHT ARROW** عندما تكون في شريط العناوين، قم بتحريك المؤشر الأيمن إلى الفاصل المنطقي التالي(. أو /)
CTRL+ENTER إضافة "**www.**" إلى بداية النص المكتوب و"**.com**" إلى نهاية النص المكتوب في شريط العناوين
UP ARROW تحريك إلى الأمام عبر قائمة متطابقات **AutoComplete**
العمل مع المفضلة
اضغط هذا للقيام بـ
CTRL+D إضافة الصفحة الحالية إلى المفضلة
CTRL+B فتح مربع الحوار **Organize Favorites**
ALT+UP ARROW تحريك العنصر المحدد إلى الأعلى في قائمة المفضلة في مربع الحوار **Organize Favorites**
ALT+DOWN ARROW تحريك العنصر المحدد إلى الأسفل في قائمة المفضلة في مربع الحوار

Favorites Organize

تحرير
اضغط فوق للقيام بـ
CTRL+X إزالة العناصر المحددة ونسخها في الحافظة
CTRL+C نسخ العناصر المحددة إلى الحافظة
CTRL+V إدراج محتويات الحافظة عند الموقع المحدد
CTRL+A تحديد كل العناصر على صفحة ويب الحالية

الموضوع التاسع عشر : اختصارات وأوامر في الدوس

- أمر **ping** : شكله **ping ip_address** مثال **ping 192.168.3.13** :
هذا الأمر يختبر الاتصال بينك وبين الجهاز آخر " فهنا مثلا سوف يقوم بالتأكد من انك متصل بالجهاز الذي يحمل هذا العنوان 192.168.3.13 " وهذا الأمر تقوم فكرته علي إرسال دفقه من المعلومات إلى الجهاز الهدف ولو قام الجهاز الهدف

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

بالرد تعرف أن الاتصال بينك وبينه قائم فعلا2-وله فائدة آخر يختبر كفاءة جهازك ووصلاته وان برتوكول **TCP/IP** مركب بطريقه صحيحه في الجهاز ، و ممكن تحل به بعض المشاكل في جهازك وتكون صورته بالشكل **Ping 127.0.0.1** وهنا سوف يقوم باختبار جهازك ولكن لماذا اخترنا هذا العنوان بالذات هذا ما سوف نعرفه عندما نقوم بشرح **IP ADDRESS3**-وله فائدة أخرى يعرفها الهاكر فلو قام جهازك بإرسال كميه مثبتة من هذه البيانات بشكل مثبت وقام عدد كبير من الأشخاص بهذا سوف يقع "أي لا يعمل لجزء من الوقت" السرفر الذي يحمل هذا العنوان ولكن سوف نضيف جزء آخر بسيط للأمر ليقوم بإرسال هذه البيانات بشكل مستمر **PING -T IP_ADDRESS** سوف تظهر لك النتائج استخدام هذا الأمر بهذا الشكل :

DATA PINGING 192.168.3.13 WITH 32 BYTES OF

MS TTL10>REPLY FROM 192.168.3.13: BYTES=32 TIME

ومن فوائده أيضا أن تعرف أل **IP address** لدومين والعكس الدومين الخاص بـ**Address IP**

عندما اكتب **Ping http://www.islamway.co**/ تكون النتيجة

/Ping http://www.islamway.com [66.33.50.23

وعندما اكتبه هكذا **ping -a 66.33.50.23** تكون النتيجة أيضا

http://www.islamway.com/ [66.33.50.23 Ping

- أمر **TRECERT** : شكله **TRECERT IP_ADDRESS** مثال **TRECERT 192.168.3.13** أو **TRECERT**

/http://www.islamway.com

وهو هنا يقوم بتتبع بعث المعلومات لك وعدد النقاط **(HUBS) (NUDS)** التي مر بها والعناوين **IP-address** الخاصة بها.

- أمر **netstat** : شكله **netstat -A**

وهو يوضح لك عنوانين الكمبيوترات التي تقوم بالاتصال بك الآن بمعني أنى أكون فاتح صفحة مجلة الفلاش سوف يخبرني أن هناك اتصال ما بي جهازي والسرفر الخاص بالمجلة.

وتظهر النتيجة بالشكل هذا مثلا

local address foreign Address State Proto

established TCP x0k8n7: 1028 205.188.7.198:5190

طبعا **TCP** هو البرتوكول المستخدم في الاتصال

و **x0k8n7** هو اسم الجهاز الخاص بيو رقم 1028 هو البورت الموجود في جهازي الذي يقوم بالاتصال والرقم 205.188.7.198 هو العنوان الخاص بالجهاز الذي اتصل به والرقم 5190 هو البورت الذي يفتحه هذا الجهاز للاتصال معي **established** معناه أن الاتصال فعلا قائم الآن جزء أخيرا إذا أردت أن تعرف أل **IP-address** لشخص أن تتحدث معه في أل **icq** ببساطه شوفه اسمه واعرف ثم اكتب الأمر **Netstat** واكتب كل البورتات والعنوانين المكتوبة

ثم أرسل له رسالة واكتب الأمر مرة ثانيه العنوان الزائد هو عنوان هذا الشخص أما إذا أردت أن تعرف عنوان شخص تتحدث معه في أل **AOL** ببساطه اعمل معه **Connection direct** مثلا لإرسال صورة أو محادثة صوتيه واكتب الأمر وسوف تجد **IP ADDRESS** أمام البورت 5190 هذا هو العنوان الخاص بالشخص الذي تتحدث معه.

- أمر **ipconfig** وهو لمعرفة العنوان الخاص بي الآن علي النت

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

وسوف يستعرض

1- **IP ADDRESS**

2- **SUBNET MASK**

3- **DEFAULT GATEWAY**

ملاحظات :

للوصول لمحث الدوس- في و ندوز أن تي و 98 و 95 **Prompt start programs MS-DOS**

أما في وندز 2000 وملنيوم **Prompt start program accessories MS-DOS**

الموضوع العشرين : وظائف كنترول (Ctrl)

الحروف التي تستخدم مع (**Ctrl**)

المفتاح العمل الذي يؤديه

Ctrl+A تحديدكامل النص

Ctrl+C نسخ التحديد سواء كان نص او صورة

Ctrl+V لصق التحديد سواء كان نص او صورة

Ctrl+X قص التحديد سواء كان نص او صورة

Ctrl+D حفظ الموقع بالمفضلة

Ctrl+F للبحث عن كلمة بالصفحة

Ctrl+Z التراجع عن آخر عمل تم تنفيذه

Ctrl+S حفظ العمل الذي تقوم به (لا يعمل مع المتصفح)

Ctrl+P تشغيل أمر الطباعة

Ctrl+W إغلاق النافذة المفتوحة

Ctrl+O فتح ملف

Ctrl+B إستخدامه مع المتصفح يفتح لك نافذة ترييب المفضلة

Ctrl+Esc الانتقال بين نافذتين أو أكثر بطريقة سريعة

الموضوع الواحد والعشرين : 31 سبباً لرسائل الأخطاء في جـهـازكـ

1-التحميل لبعض البرامج والغير مهمة

2 - عدم توافق بعض الكروت داخل الجهاز

3 - كثرة الكروت المركبة بالجهاز ، وخاصة كرت الفيديو ، والسيدي رايتر

4 - وجود أخطاء أو عطب في إحدى ملفات النظام المحمل على جهازك

5 - إختلاف الرامات المركبة بالجهاز حيث لا يتم التوافق بينها فهي سبب في حدوث المشاكل

6 - من الممكن وجود أخطاء تـقـنية في اللوحة الأم وخاصة مداخل الكروت والرامات

7 - برنامج زون الارم إذا لم يبرمج صح فله تأثير في ذلك

8- تحيل صفحات الأنترنيت دون إتصال

9- تصفح الصفحات السوداء والغامقة جداً

سيف علي حسن الدار

aldare-1989@hotmail.Com

+967/ 771323146 -735446181

saif201028@yahoo.com

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

10- فتح الميكروسوفت وورد أثناء التصفح
11 - التنقل السريع بين النوافذ المفتوحة من الأنترنيت
12- برنامج النورتن إنتي فايروس إذا لم يتم تثبيته بشكل سليم
13- فتح البرامج المنزلة أثناء تصفح الأنترنيت
14 - برنامج القيت رايت له دور في تلك المشكلة
15 - كثرة الإرتباطات التي تخرج فجأة عليك أثناء التصفح
16- ضغط الكمبيوتر بفتح النوافذ
17 - فتح الملفات المرسلة من قبل الماسنجر
18 - فتح المواقع المخلة بالشرف (المواقع ال***ية) فهي الأكثر بخروج المشاكل
19 - ضغط الهاردسك بتنزيل البرامج عليه
20 - كثرة تحميل الصور من مواقعها
21- وجود فيروسات داخل الجهاز
22- عدم تحديدث النورتن إنتي فايروس بشكل دوري
23- عدم معالجة الأخطاء في وقتها عن طريق البحث عنها وتركها تتراكم في الجهاز
24- تنصيب ويندز على ويندز دون الفرمته والمسح والتنزيل من جديد
25- تشغيل بعض أنواع الأقراص المضغوطة حيث بعضها غير سليم
26 - بعض أنواع اقراص الويندز لاتكون مكتملة البرامج أثناء تحميلها للتنصيب
27 - عدم القيام بتشغيل معالجة الصيانة للجهاز بصفة شبه يومية
28- عدم حذف ملفات الأنترنيت المؤقتة وجعلها تتراكم دون التخلص منها
29 - عدم حذف ملفات المحفوظات وجعلها تتراكم دون حذفها و التخلص منها
30 - عدم تفحص الأقراص وتنظيفها والقيام بعملية التجزئة بشكل شبه يومي
31- تشغيل الريل بلير لأستماع الأصوات أثناء تصفح الأنترنيت له أيضاً دور في ذلك

الموضوع الثاني والعشرين : طريقة معرفة إذا كان جهازك مخترق

أو لا تذهب لقائمة ابدأ ثم لـ البرامج وتذهب لبرنامج الدوس
ومنها اختره ... بعده يطلع لك مربع اسود وفيه كلام هذه هي شاشة الدوس بعد ذلك اكتب هذا الامر **netstat –a**
نلاحظ أن هناك مسافة بين الكلمه والشرطه ، ثم اضغط انتر **Enter** سيقوم البرنامج بعرض جميع الاتصالات التي حدثت مع جهازك
اذا وجدت جميع الارقام التي ظهرت لك أصفار مثل 00.00.00.0 فمعناها ان جهازك لم يتصل بأي جهاز اخر او خط اخر ، واذا كان متصلا مع احد فسيظهر لك مع القائمه مثلا 168.167.240.32:1243
فاذا رأيت مثل هذا اعلم ان جهازك متصل مع شخص ما
عن طريق البورت 1243

الموضوع الثالث والعشرين : نبذة عن نظام التشغيل

لسنا بصدد طرح نبذه تاريخيه عن نظم التشغيل بامكانك بسهولة الحصول عليها
لكن ندخل في تفاصيل نظم التشغيل وسأقوم بالتركيز على عده امور منها:

سيف علي حسن الدار
+967/ 771323146-735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

1.المقاطعات. **interrupt**
2.ماذا يفعل نظام التشغيل عندما تبدأ بفتح جهازك
1.المقاطعات: **interrupt**
ملاحظات مهمه:
كل جهاز كمبيوتر يحتوي على نظام تشغيل على الاغلب يوجد في اول كيلو بايت من الذاكره **memory** ما نسميه
interrupt vector table
ماهي **interrupt vector table** هي عبارة عن مصفوفه ان جاز القول تحتوي على **numbers** تحدد كل منها ما هو الجهاز على سبيل المثال
int 0 المقاطعة رقم صفر: تدل على الوقت في الكمبيوتر اي انها تخدم الوقت
int 1 المقاطعة رقم 1 : تدل على لوحة المفاتيح
وهكذا....................حتى تكتمل جميع الاجهزة(ماوس وسكانر وكرت شاشه الخ)
لماذا نظام المقاطعات:
قديما لم يوجد هذا النظام بل كان **cpu** يقو بسؤال الاجهزة واحد تلو الاخر اذا اراد خدمه ان ينفذها له على سبيل المثال:
يقوم **cpu** بسؤال لوحة المفاتيح اذا اردت شيء (مثلا كتابة حرف على الشاشة)
ثم يذهب مباشرة للطباعة اذا اردت شيء....ثم يذهب فرضا الى الماوس وهكذا
فان **cpu** كل الوقت يذهب للسؤال الاجهزة اذا اردت خدمة وهذا يضيع عمل **cpu** الاصلي القائم على تنفيذ البرامج....تصور انك تريد تحميل برنامج بهذه الطريقة ستحتاج الى وقت كبير جدا لترى النتائج وهذه مشكلة كبيرة جدا......
علاوة فرضا قمت بتنفيذ برنامج معين وهذا البرامج يطلب من المستخدم ادخال قيم معينه)**i\o**) فان **cpu** سينتظر

المستخدم حتى يدخل القيم وهذه مشلة لان وقت **cpu** سيضيع من جراء الانتظار...................... لذلك جاء مفهوم المقاطعة :
وهي ان **cpu** يقوم بتنفيذ البرامج واذا اراد اي جهاز ان خدمة **service** من **cpu** فانه يقوم باعلامه ومن ثم يقوم **cpu** بخدمته..... وبالتالي اذا طلب برنامج اي قيم لادخالها فان **cpu** لا ينتظر بل يذهب لتنفيذ برامج اخرى وهذه فائده كبرى ....اذاادخل المستخدم القيم يعود **cpu** ويكمل عمل البرامج............

كيف تعمل المقاطعة:
اولا سوف ابسط الامر على الرغم من تعقيده سأناقشه بطريقة سطحية ولكن كافيه
اولا قطعة تسمى **pic** المقاطعات المبرمجة وهذه تكون كل اجهزة الكمبيوتر موصولة بها(ماوس لوحة مفاتيح.......)
وتكون موصوله بها عن طريق ما يسمى **irq** اذا على سبيل المثال لوحة المفاتيح موصولة مع **pic** على **irq 1**
الماوس موصولة مع **pic** على **irq 2** وهكذا.......باقي الاجهزة والمكونات طبعا **cpu** غير موصول فهو رئيسي بالكمبيوتر ولا يحتاج الى خدمات بل هو من ينفذ الخدمات.....
كيفية العمل:
لنفترض نريد كتابة حرف **A** على الشاشة عند الضغط على الحرف ماذا يحصل.......
اولا تقوم لوحة المفاتيح بمقاطعة **pic** عن طريق **irq** بحيث تزيد في فولتية القطعة ومن هنا تعرف **pic** ان لوحة المفاتيح تريد خدمة تقوم ال **pic** (المقاطعات المبرمجة) بارسال مقاطعة ل **cpu** والذي بدوره يسئل من احدث هذه

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146 -735446181
saif201028@yahoo.com

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

المقاطعة ما هو رقم المقاطعة بطريقة او باخرى فتقوم قطعة **pic** باعطائة الرقم
يقوم **cpu** بزيارة **interrupt vector table** ويضع الرقم الذي اراد المقاطعة فيجد انه لوحة المفاتيح.......
بعد ذلك يقوم **cpu** بخلق مقاطعة تسمى مقاطعة رقم 19 وهذه المقاطعة مسؤولة لمعرفة ماذا تريد لوحة المفاتيح ......
مقاطعة رقم 19 تعمل التالي : تذهب الى **bios segment** وتذهب بلاخص الى محل تخزين لوحة المفاتيح(اذ ان حرف **A** الذي كتبته يخزن هنالك) **buffer keyboard** اذا كان المضغوط في لوحة المفاتيح هو **crtl + alt +del** حتى يعمل عملية **restart** اعادة التشغيل يجد انه لا ليس هو المضغوط يذهب الى **function key** مثل مفتاح الشفت **shift crtl alt capslock** وهكذا (لكتابة حرف **A** اما نقوم بضغط **shift a** او بضغط مفتاح **capslock**) لنفترض
ان مفتاح **shift** هو المضغوط بالتالي كل حرف في الكمبيوتر يمثل بسبعة **BIT(BIT** اصغر وحده مساحة بالكمبيوتر
اذا كان اخر بت رقم سبعه مضاء يعني موضوع 1 هذا يعني انه هناك **FUNCTION KEY** مضغوط بالتالي يفحص ويجد انه **SHIFT** بالتالي يذهب مباشرة الى المكان الذي تخزن فيه احرف لوحة المفاتيح ويجد حرف **a** فيجعله **A** ....

اما عملية الطباعة على الشاشة فانه عبر اوامر وهي مقاطعات تنفذ هذه الاوامر على كل الاحوال يوضع حرف **A** على موقع كرت الشاشة مباشرة في الذاكره فيعرض بصورة سريعة............

هذا ما يدور اذا اردت كتابة حرف **A** الف من العمليات من اجل حرف ولكن كل هذه العمليات لا تتعدى اجزاء من الثانية ....
2.ماذا يفعل نظام التشغيل اذا شغلت الجهاز:::!!!!
والذي بدوره يعمل على تعريف جميع الاجهزة المتوفرة ثم يقوم بتحميل **command .com** ثم في خدمة المستخدم

الموضوع الرابع والعشرين : أفكـار الكمـبيوتـر والإنـتـرنـت

إليكم هذهي الإكتشافات المفيدة لإختصار الوقت لدى تصفحكم على صفحات الأنترنت فقط وهي : -
1 - إضغط على **F11** مرة واحدة أثناء التصفح ولاحظ النتيجة ، وللعودة إضغط مرة أخرى 0
2 - إضغط على **F2** للحصول على معلومات قد أنت بحاجة إليها 0
و إليكم هذهي الإكتشافات المفيدة لإختصار الوقت أثناء عملكم على صفحات الكمبيوتر أو تحرير صفحات فقط وهي : -
1 - ضع الممحات (المساحة) على الخط المطلوب مسحه في جدول ما قمت بتصميمه ، ثم إضغط الماوس الأيسر مرة واحدة ثم لاحظ
حصول النتيجة 0
2 - إضغط على **F1** للحصول على إظهار المساعد 0
3 - إضغط على **F4** لتكرار ونسخ ما قمت به من عمل كتابي في السطر نفسه 0
4 - إضغط على **F5** لعملية البحث والإستدلال 0
5 - إضغط على **F7** لعملية التدقيق الإملائي 0

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

6 ـ إضغط على **F8** لإيقاف عملية الكتابة من شخص آخر ، وللعودة إضغط على تراجع 0
7 ـ إضغط على **F10** لعملية إيقاف حركة المؤشر إثناء النسخ 0
8 ـ إضغط على **F12** لعملية الحفظ بإسم

الموضوع الخامس والعشرين : ماهو الإنترنت وتاريخه

ماهي الانترنت

الانترنت هي عبارة عن شبكة كمبيوترات ضخمة متصلة مع بعضها البعض. وتخدم الانترنت أكثر من 200 مليون مستخدم وتنمو بشكل سريع للغاية يصل إلى نسبة 100% سنوياً، وقد بدأت فكرة الانترنت أصلاً كفكرة حكومية عسكرية وامتدت إلى قطاع التعليم والأبحاث ثم التجارة حتى أصبحت في متناول الأفراد. والانترنت عالم مختلف تماماً عن الكمبيوتر، عالمٌ يمكن لطفل في العاشرة الإبحار فيه. ففي البداية كان على مستخدم الانترنت معرفة بروتوكولات ونظم تشغيل معقدة كنظام تشغيل **Unix** أما الآن فلا يلزمك سوى معرفة بسيطة بالحاسب لكي تدخل إلى رحاب الانترنت. كما كان في الماضي من الصعب الدخول للانترنت خلال الشبكة الهاتفية باستخدام مودم ولكن مع انتشار شركات توفير الخدمة تبددت هذه الصعوبات، فمنذ أن بدأت شركة **CompuServe** توفير خدمة الدخول على الانترنت بواسطة الشبكة الهاتفية عام 1995 عبر بروتوكولات **Point-to-Point** لم يعد الدخول في الانترنت أمراً صعباً. وأهم عناصر الانترنت الرئيسية هي (أ) الشبكة العنكبوتية **www** (ب) نقل الملفات **FTP** (جـ) البريد الالكتروني **E-Mail** (د) مجموعات الأخبار **Usenet**. أهم ما يجب أن تعرفه عن الانترنت هو أنها تعتمد اللغة الإنجليزية كلغة رسمية وأن الإبحار في الانترنت مجاني تماماً ولكن الثمن الذي تدفعه هو لتوفير الخدمة لك.

تاريخ الانترنت

الخمسينيات

1957 الاتحاد السوفيتي يطلق **Sputnik** أول قمر صناعي. ردت عليه الولايات المتحدة بتأسيس (وكالة مشروع الأبحاث المتطورة) (**Research Project Agency Advanced**) اختصاراً (**ARPA**) بتمويل من وزارة الدفاع الأمريكية.

الستينيات

1967 أول ورقة تصميم عن **ARPAnet** تنشر بواسطة لورنس روبرت.

1969 **ARPAnet** تؤسس بتمويل من وزارة الدفاع لإجراء بحوث عن الشبكات. تم إنشاء أربعة مفاصل **Nodes**.

السبعينيات

1970 تأسيس **Alohanet** بجامعة هاواي.

1972 **Alohanet** ترتبط بـ **ARPAnet**.

1972 ري تاملنسون اخترع برنامج البريد الالكتروني لإرسال الرسائل عبر الشبكات الموزعة.

1973 أول اتصال وربط دولي مع **ARPAnet** وذلك مع جامعة كلية لندن **University College of London**.

1974 **BBN** تدشن **Telnet** وهي نسخة تجارية لـ **ARPAnet**.

1974 **Vint Cerf** و **Bob Kohn** ينشران تصميماً لبروتوكول يسمى **TCP**.

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

الثمانينيات

1981 **Minitel** و **Teletel** تنتشر في فرنسا بواسطة **France Telecom**.

1982 **DCA** و **ARPA** يؤسسان (**TCP**) أي **Protocol Transmission Control** و (**IP**) أي **Internet Protocol** وبذلك أصبحت (**TCP/IP**) اللغة الرسمية للانترنت.

1982 **EUnet** أسست بواسطة **Euug** لتقدم خدمة البريد الالكتروني ومجموعات الاخبار.

1982 مصطلح (انترنت) يستخدم لأول مرة.

1983 تطوير ما يسمى بـ @_@@_@@_@@_@ **Server** في جامعة ويسكنسن.

1984 تم تطوير **DNS** أي **Server @_@@_@@_@@_@ Domain** وتجاوز عدد النظم المضيفة (**Hosts**) ما يقارب 1000 جهاز.

1987 تجاوز عدد النظم المضيفة 10000 جهاز.

1987 اتحاد شركات **Merit** و **IBM** و **MCI** لتكون شركة **ANS** والتي قامت بتقوية اتصالات الشبكة واجهزتها ثم فتح الخدمة في الدول الحليفة لأميركا.

1989 تجاوز عدد النظم المضيفة 100000 جهاز.

1989 تكوين (وحدة مهندسي الانترنت **IETF**) و (وحدة باحثي الانترنت **IRTF**) تحت اشراف **IAB**.

1989 ارتبطت كل من (استراليا، المانيا، اسرائيل، ايطاليا، اليابان، المكسيك، هولندا) بشبكة**NSFNET**.

التسعينيات

1990 نشأت **Archie**.

1990 أصبحت شركة **The World Comes On-line** أول شركة تجارية توفر خدمة الانترنت.

1991 تونس ترتبط بالانترنت كأول دولة عربية ترتبط بالشبكة.

1991 نشأت **WAIS** و **Gopher** و **WWW**.

1992 تأسست جمعية الانترنت **Internet Society** وتجاوز عدد النظم المضيفة مليون.

1992 الكويت ترتبط بالانترنت.

1992 البنك الدولي يرتبط بالانترنت.

1993 البيت الأبيض والأمم المتحدة يرتبطان بالانترنت.

1993 مصر والإمارات ترتبطان بالانترنت.

1993 انتشر **Mosaic** و **WWW** و **Gopher** بشكل واسع جداً.

1994 انتشار التسوق على الانترنت والشركات تدخل الشبكة بشكل واسع.

1994 لبنان والمغرب ترتبطان بالانترنت.

1995 **CompuServe** و **America On-line** و **Prodigy** تعمل لتوفير الخدمة للمشتركين.

1995 طرح **JAVA** في الأسواق.

1996 انعقاد أول معرض دولي للانترنت.

1996 قطر وسوريا ترتبطان بالانترنت.

1999 المملكة العربية السعودية ترتبط بالانترنت

من يدير الانترنت

سؤال قد يتردد كثيراً ،، وكثير من الناس تعتقد بأن هناك جهة تمتلك الانترنت وذلك غير صحيح! وهذا من أكثر الأشياء

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

التي تدعو للاستغراب، وإن كان أقرب شيء يشبه السلطة الإدارية في الانترنت هي جمعية الانترنت **ISOC** وهي جمعية غير ربحية لأعضاء متطوعين يقومون بتسهيل ودعم النمو الفني للانترنت وتحفيز الاهتمام بها. فكل مستخدم للانترنت مسؤول عن جهازه، وهناك ما يسمى بالعمود الفقري للانترنت وهو الجزء الرئيسي للشبكة الذي ترتبط به شبكات أخرى وعند إرسال معلومات يجب أن تمر بهذا العمود الفقري. ويلي ذلك الشبكة الوسطى للانترنت وهي شبكة العبور التي تربط الشبكة الجذرية بالعمود الفقري أي تقوم بربط مناطق جغرافية بالعمود الفقري، والشبكة الجذرية هي المستوى الثالث من الانترنت وتقوم بربط شبكات المؤسسات والمعاهد بشبكات المناطق الجغرافية في المستوى المتوسط والذي يسمح لهم بالدخول على العمود الفقري. ولا أحد يقوم بتمويل كل ذلك بل إن كل شركة مسؤولة عن تمويل نفسها.

نشأة الانترنت **HTML** تعليم لغة الاختراق السرية في الانترنت الكمبيوتر المثالي **FTP** نقل الملفات **USENET** تلميحات مصطلحات شائعة مواقع انترنت

<u>الموضوع السادس والعشرين : أعرف كل أدق التفاصيل عن نوعيـة الملفات في جهازك</u>

في جهاز الكمبيوتر توجد عدة أنواع من الملفات المختلفة ، ولكل ملف اسم يتكون من مقطعين كما نرى هنا:

setup.exe

المقطع الأول هو اسم صغير يصف الملف (وهو هنا **setup**) ، والمقطع الثاني يدعى امتداد الملف ويتكون في الغالب من ثلاثة أحرف (وهو هنا **exe**) ، وهذا الامتداد يميز نوع الملف ، وهو جوهر ما نتحدث عنه. ويفصل بين المقطعين النقطة(.)

في نظام ويندوز يكون لأغلب أنواع الملفات الموجودة بالجهاز ما يسمى بالاقتران ببرنامج معين ، وكذلك يوجد رمز يتبع هذا الاقتران ، ونلاحظ ذلك في ملفات برنامج **MS Word** مثلاً فملفاته تدعى بالمستندات وتنتهي بالامتداد **doc** ولها رمزها الخاص (وهو في ملفات **Word** يشبه حرف **W** على ورقة) وفي معظم الأحيان يقوم نظام ويندوز بإخفاء امتداد الملفات المعرفة للنظام باقتران ببرنامج معين ورمز ، لذلك يلاحظ أن الملفات المجهولة تكون ذات رمز مثل ورقة بداخلها شعار ويندوز (النافذةالملونة) ويظهر امتدادها ، وعند محاولة فتحها يظهر مربع حوار "فتح بواسطة **Open With**" وبداخله قائمة بعدة برامج مقترحة لأن تفتح الملف بواسطتها.

وإذا أردت رؤية قائمة بأنواع الملفات المقترنة والمعرفة في النظام ففي ويندوز 95 اختر قائمة عرض **View** من أي مجلد تكون فيه ، واختر إعدادات **Options** ومنها اختر علامة تبويب أنواع الملفات **File Types** وسترى قائمة بانواع الملفات المعرفة للنظام ، وفي ويندوز 98 فاختر من قائمة ابدأ **Start** قائمة الإعدادات **Settings** ومنها **Folder Options** وهناك تأخذ علامة التبويب أنواع الملفات **File Types**.

كذلك يمكنك التحكم بظهور الملفات من نفس مربع الحوار في النظامين 95 و 98 بأخذ علامة التبويب عرض **View** ، وفيها يمكن مثلاً إظهار جميع المفات ، حيث يكون في الإعدادات الافتراضية أن الملفات المخفية **hidden files** لا تظهر للمستخدم في المجلد ، لكن عند تحديد هذا الاختيار تظهر الملفات المخفية بشكل شفاف للمستخدم.

كذلك يمكن إظهار امتدادات الملفات المعرفة أيضاً وغيرها من الإعدادات.

و تجد هنـــا قائمة بأنواع أكثر الملفات استخداماً

ملفات صور مختلفة منها متحرك **jpg-gif-bmp-tif-psd-wmf-psp-aif-jpe**

ملفات صوتية وميديا **mid-rmi-wav-mp*-rm-ra-au-snd**

ملفات مضغوطة **zip-cap-rar-arj-tar-Z**

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

ملفات نظامية وملفات تشغيل **sys-dll-vxd-drv-ini-inf-ocx**
ملفات نصية **wri-txt-pdf**
ملفات برامج أوفس **doc-xl*-ppt-pps-mdb-md***
ملفات خطوط **fot-ttf-tff-fon**
صفحات وملفات إنترنت **htm-html-js-pl-cgi-asp-shtml**
ملف تنفيذي - برنامج **exe**
ملف مساعدة **hlp**
ملف شاشة توقف **scr**
ملفات فيديو **avi-mp3-rm-smi-qt-mov**
ملفات رموز ومؤشرات للفأرة **ani-cur-ico**

الموضوع السابع والعشرين : أوامر مهمه جداً للويندوز

موضوع اليوم عن أوامر مهمة جداً للويندوز تستطيع من خلالها تشخيص مشاكل الجهاز والاستفادة من قدرات الجهاز ..... إلخ
وقبل أن ابدأ أود التنويه على أنه قبل أن تبدأ بعمل الأمر لابد أن تضغط (إبدأ) ثم (تشغيل) ومن ثم تقوم بكاتبة أحد هذه الأوامر ومع كل أمر تجد الشرح أسفل القائمة المسندلة هذه وإليكم الأوامر بالتفصيل ....
أولا اذهب إلى ابدأ **star** ثم تشغيل **run** ثم اكتب الأمر الذي تريد من هذه الأوامر التي أمامك ...
Winipcfg هذا الأمر لإظهار الاي بي لجهازك.

Drwatson أداة لتشخيص أخطاء النظام
مهمته: أخذ لقطة عن النظام عند حدوث أي خطأ فيه. وتعترض هذه الأداة أخطاء البرنامج، وتعرّف البرنامج الذي أخطأ، وتقدم وصفاً مفصلاً لسبب الخطأ. وبإمكان **Dr. Watson** في أغلب الأحيان تشخيص المسألة واقتراح سير الإجراءات. وعند اتصالك بالدعم الفني في **Microsoft** للحصول على المساعدة، فإن **Dr. Watson** هو الأداة المستخدمة لتقييم المشكلة.
Msconfig هذا الأمر لأدوات النظام وشاشة بدء التشغيل.
مهمة الأداة المساعدة لتكوين النظام هي :
تقوم الأداة المساعدة لتكوين النظام (**Msconfig.exe**) بأتمتة الخطوات الروتينية لاستكشاف الأخطاء وإصلاحها التي يتّبعها مهندسو الدعم الفني في **Microsoft** عند تشخيص مسائل تتعلق بتكوين **Windows** **98.**
وتسمح لك هذه الأداة بتعديل تكوين النظام من خلال عملية حذف خانات الاختيار، وتقليل المجازفة بكتابة أخطاء مقترنة بشكل مسبق بالمفكرة ومحرر تكوين النظام.
كما أنه بإمكان الأداة المساعدة لتكوين النظام إنشاء نسخة احتياطية عن ملفات النظام قبل أن تبدأ جلسة العمل المخصصة لاستكشاف الأخطاء وإصلاحها. وعليك إنشاء نسخ احتياطية عن ملفات النظام لضمان إمكانية عكس التعديلات التي تم إدخالها أثناء جلسة العمل المخصصة لاستكشاف الأخطاء .
للحصول على مزيد من المعلومات حول استخدام الأداة المساعدة لتكوين النظام، انقر فوق تعليمات في إطار الأداة المساعدة لتكوين النظام.

سيف علي حسن الدار
+967/ 771323146-735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

Regedit هذا الأمر للوصول إلى الرجستري لعمل بعض التعديلات التي تريدها.
Command هذا الأمر يقوم بتشغيل شاشة الدوس.
CLEANMGR.EXE هذا الأمر لتنظيف الأقراص فقط، حدد محرك الإقراص المراد تنظيفه ثم اضغط على موافق.
Defrag هذا الأمر لعمل تجزئة القرص الصلب.. عند استخدامه اضغط على إعدادات للاطلاع على الخيارات المتاحة أو لتعديلها حسب رغبتك .
ScanDisk هذا الأمر للتدقيق في الجهاز من ناحيتي الملفات والنظام بحثا عن الأخطاء وإصلاحها.
انقر فوق محرك الأقراص الذي يحتوي على الملفات والمجلدات التي تريد التدقيق فيها، تحت نوع الاختبار، انقر فوق قياسي، ثم انقر فوق البدء.
CVT1.EXE هذا الأمر لتشغيل معالج محول محركات الأقراص إلى نظام **fat32** يقوم محول محرك الأقراص بتحويل محرك الأقراص إلى نظام الملفات **FAT32**، الذي يعتبر تحسيناً لجدول تخصيص الملفات (**FAT** أو **FAT16**) وهو تنسيق
نظام الملفات. وعندما يكون محرك الأقراص في هذا التنسيق، فهو يخزّن البيانات بفعالية أكبر، وذلك بإنشاء عدة مئات ميغابايت من المساحة الإضافية على محرك الأقراص. وبالإضافة إلى ذلك، فإن تشغيل البرامج يتم بشكل أسرع ويستخدم الكمبيوتر موارد نظام أقل.
SCANREG مدقق تسجيل ويندوزلتفحص التسجيل
وظيفته: يحتفظ نظامك دوماً بنسخة احتياطية عن تكوين التسجيل بما فيها (معلومات عن حساب المستخدم، وروابط البروتوكول، وإعدادات البرامج، وتفضيلات المستخدم). ويمكنك استخدام النسخة الاحتياطية إذا صادف التسجيل الحالي مشكلة.
وفي كل مرة تعيد فيها تشغيل الكمبيوتر، يقوم مدقق التسجيل تلقائياً بتفحص التسجيل. إذا لاحظ مدقق التسجيل وجود مشكلة، فهو يستبدل تلقائياً التسجيل بالنسخة الاحتياطية. إذا احتوى التسجيل على إدخال يشير إلى ملف لم يعد موجوداً مثل ملف (**vxd**)،
فلن يتم تصحيحه بواسطة مدقق التسجيل.
Tune up هذا الأمر لتشغيل معالج الصيانة ومن مهامه:
1/ تسريع البرامج المستخدمة بشكل متكرر
2/ تدقيق القرص المثبت لاستكشاف الأخطاء
3/ حذف الملفات الغير ضرورية من الجهاز
ويمكن استخدام هذا الأمر لنفس الغرض **TUNEUP.EXE**
SIGVERIF أداة التحقق من التوقيع لـ**Microsoft** تبحث أداة التحقق من التوقيع عن الملفات الموقعة وغير الموقعة على الكمبيوتر.
الملف الموقع هو الملف الذي تم منحه توقيعاً رقمياً من **Microsoft**. ويفيد التوقيع بأن الملف عبارة عن نسخة غير معدّلة من الملف الأصلي. ويمكنك بواسطة أداة التحقق من التوقيع القيام بما يلي: عرض شهادات الملفات الموقعة للتأكد من عدم التلاعب بها. البحث عن ملفات موقعة في موقع معيّن. البحث عن ملفات غير موقعة في موقع معيّن
SYSEDIT محرر تكوين النظام لا ينصح بتغيير أي شيء فيها إلا من قبل الخبراء أو من لديهم معرفة تامة بالتعديلات التي يريدون عملها على هذا المحرر.
SFC يمكنك استخدام مدقق ملفات النظام للتحقق من تكامل ملفات نظام التشغيل، ولاستعادتها إذا كانت معطوبة،

سيف علي حسن الدار
aldare-1989@hotmail.Com
+967/ 771323146-735446181
saif201028@yahoo.com

ولاستخراج الملفات المضغوطة(مثل برامج التشغيل) من أقراص التثبيت.
VCMUI أداة تعارض الإصدارة وظيفتها التحقق من الملفات التي لديها رقم إصدارة احدث أو كانت بلغة مختلفة قبل تثبيت النظام لاستعادتها

شرح مبسط عن هذه الأداة:
أثناء تثبيت برامج جديدة، بما فيها **Windows 98**، قد يتم الكشف عن الإصدار القديمة لملفات البرامج واستبدالها بالإصدار الجديدة. ويتم إنشاء نسخة احتياطية للإصدارات السابقة وتُحفظ على القرص المثبت. في حال وجدت تعارضات مع ملفات النظام أو ملفات البرامج بعد تثبيت تطبيق، تُستخدم إدارة تعارض الإصدار لاستعادة ملف النسخة الاحتياطية. وتذكر إدارة تعارض الإصدار كافة ملفات النسخة الاحتياطية، وتاريخ إجراء النسخة الاحتياطية، وأرقام الإصدار لملفات النسخة الاحتياطية والملفات الحالية. وعند استعادة ملف النسخة الاحتياطية، حينئذ، يتم إنشاء نسخة احتياطية للإصدار الحالي. ويبقى الإصداران متوفرين.
ملاحظة مهمة : يجب استخدام هذه الأداة من قبل شخص لديه معرفة متقدمة بالنظام .
UPWIZUN إلغاء تثبيت معالج التحديث وظيفته كالتالي: ربما قد استخدمت **Windows Update** لتثبيت إصدار محدّث من أداة تصحيح، أو برنامج تشغيل، أو أداة نظام. إذا قررت فيما بعد إلغاء تثبيت الإصدار الجديد،ولم تتمكن من إعادة تأسيس الاتصال بإنترنت، استخدم إلغاء تثبيت معالج التحديث للعودة إلى الإصدار السابق.
Asd.exe أداة تشغيل عامل برنامج تشغيل التخطي التلقائي
وظيفته: يعرّف برنامج تشغيل التخطي التلقائي (**ASD**) حالات الفشل التي تسببت في توقف **Windows** عن الاستجابة في عمليات بدء التشغيل السابقة ويضع عليها علامات بحيث يتم تجاوزها في عمليات بدء التشغيل اللاحقة. يذكر **ASD** كافة الأجهزة أو العمليات التي فشل بدء تشغيلها. ويمكنك استخدام **ASD** لتمكين أي جهاز تم تعطيله سابقاً بواسطة **ASD**، وسيحاول **Windows** استخدام الجهاز في محاولة بدء التشغيل التالية. وفي حال الفشل، يتوقف الكمبيوتر عن الاستجابة. وعند إعادة تشغيل الكمبيوتر مرة أخرى، يمنع **ASD** تشغيل العملية سامحاً لك ببدء تشغيل الكمبيوتر

الموضوع الثامن والعشرين : كيف تطفي جـهـاز من يـزعـجـك فـى الكمـبـيـوتـر

اول خطوه هو ان تذهب لمكان فارغ في سطح المكتب ثم تضغط على الزر اليمين وسوف تخرج لك نافذة اختر جديد : عندما تضغط على جديد سوف يفتح لك نافذة آخرى اختر منها اختصار . **short cut** سوف يفتح لك نافذة : اكتب خلال سطر الاوامر هذي العبارة **rundll.exe user.exe,exitwindows** الافضل انسخها ثم اضغط على التالى ثم اكتب اي اسم ثم ارسل هذا الملف الى صديقك على المسنجر وحالما يفتح صديقك هذا الملف فانه مباشرة ينطفيء جهازه ملاحظة هذي الطريقة لا تضر صاحب الجهاز بل فقط تطفيه فقط وبامكانه اعادة التشغيل مرة اخرى

الموضوع التاسع والعشرين : اختـراق الشبكـات الـهـاتفـيـة

ربما يظن البعض أن الهاكرز لا يستطيعون التهكير والقرصنة إلا من خلال الإنترنت أو شبكات مماثلة في المميزات ولكن هذا غير صحيح فحتى تلك الشبكات التي لا ترتبط بالإنترنت أو بشبكات أخرى ليست في مأمن بعض الأوقات خاصة إذا كانت تحتوي على خدمات الاتصال عن بعد مثل الهاتف والاتصالات اللاسلكية.
الهاكرز يعتمدون غالبا على هذه الخدمات لاختراقهم شبكة في منطقة قريبة منهم خاصة شبكات الشركات الكبيرة والتي

ثلاثون موضوعاً مهماً في الانترنت والشبكات والحاسوب

تحتوي على ما خف حمله وغلا ثمنه وقبل القيام أو البدء بعملية الاختراق يقوم الهاكرز بجمع بعض المعلومات عن تلك الشركة المستهدفة وهذه المعلومات تكون غالبا متعلقة بأرقام هواتف الشركة والمتوفرة في أي دليل للهاتف أو من خلال استعلامات الهاتف وأيضا سيحاولون الحصول على بعض أسماء المستخدمين في تلك الشركة والمسؤول عن شبكة الشركة وقد تكون الإنترنت مفيدة في بعض الأحيان لمثل هذه الخدمات فالكثير من تلك الشركات تملك موقعا على الإنترنت للتعريف بها ومنتجاتها ومن خلال أحد المواقع التي توفر خاصية **whois** يمكن للمهاجمين الحصول على معلومات مفيدة جدا في الكثير من الحالات ولا أرغب بالتوضيح أكثر لكي لا يساء الفهم.

نعود لشبكاتنا الحاسوبية التي تستخدم خدمة الدخول عن طريق الهاتف **Dial Up** لمستخدميها إذا ما كانوا بعيدين عن مقر الشبكة ويستطيع الهاكر بلعبة سهلة أن يحصل على رقم الهاتف الذي يوفر دخولاً للشبكة الحاسوبية بمجهود بسيط جدا ولكن ربما يستغرق بعض الوقت ففي البداية يقوم الهاكر بالحصول على رقم الشركة الهاتفي الرئيسي ولنفرض أنه 1234567 ويعلم الكثيرون أن أول ثلاثة أرقام وهي 123 تكون في الغالب رمز المقسم الذي تقع في نطاقه الشركة بينما 4567 ستكون متغيرة عندئذ يلجأ المهاجم لأحد برامج طلب الأرقام الهاتفية والتعرف على المودمات من خلفها والتي يطلق عليها **War Dialers** فيطلب من هذا البرنامج الاتصال بجميع الأرقام التي تقع بين 1230000 و 1239999 أي ما يقارب 10 آلاف رقم وقد تستغرق هذه العملية حوالي 5 أيام في المتوسط أما إذا كان المهاجم يستخدم أكثر من مودم فالوقت سيكون أقل بكل تأكيد ولكن هذه العملية يلجأ إليها الهاكرز في خارج أوقات الدوام الرسمي وفي أيام العطل وذلك لتجنب أعين الرقيب وكذلك فإنهم يحاولون منع رقمهم الهاتفي من الظهور لدى الطرف الآخر إذا كان يستخدم خدمة إظهار الرقم **Caller ID** لكيلا يثيروا الانتباه وغالبا ما يلجأ المهاجمون إلى استخدام أكثر من رقم هاتفي للاتصال من خلاله لكيلا يثيروا انتباه شركة الاتصالات الخاصة بهم.وبعد حصول المهاجم على الرقم الخاص بالدخول على الشبكة يقوم بالاتصال بهذا الرقم وينتظر ليرى ما إذا كان هناك تحقق من الشخصية **User Authentication** عند الدخول (وهذا ما يحدث دائما) وعند طلب الخادم الهاتفي للشبكة منه إدخال اسم المستخدم الخاص به فإنه يقوم بتجربة لائحة أسماء المستخدمين العاملين في الشركة والتي حصل عليها في وقت سابق وإذا لم يكن يملك مثل هذه اللائحة فإنه يقوم بتجربة بعض الأسماء المعروفة والتي تعمل مع الخادم الهاتفي بشكل قياسي مثل **guest** و **anonymous** و **admin** و **administrator** و **root** والتي يغفل عن إغلاقها مديرو الشبكات غالبا.

وإذا لم يستطع المهاجم الولوج للشبكة باستخدام إحدى الطرق السابقة فإنه يلجأ لحيلة قديمة ولكنها فعالة دائما وهي أن يقوم بإرسال بريد إلكتروني للمستخدمين متظاهرا فيه بأنه مدير الشبكة ويطلب منهم تزويده باسم مستخدم **User** @_@@_@@_@@_@ وكلمة سرية جديدة بالإضافة إلى الاسم القديم والكلمة السرية الخاصة به وذلك لغرض عمل الصيانة للشبكة وكي لا يفقد المستخدم حسابه.. أرجو أن تكون قد فهمت المغزى من هذه الرسالة للمستخدمين عزيزي القارئ.

وبالطبع فغالبا ما يقوم أحد المستخدمين بالرد على الرسالة البريدية بالمعلومات المطلوبة وهنا يكشر المهاجم عن أنيابه فرحا بغباء أحدهم وسيتمكن بنسبة 98% من الدخول للشبكة وسرقة جميع ما تحتويه من وثائق ومعلومات وستتكلل عمليته بالنجاح أما 2% الباقية للفشل فهي احتمال أن يكون مدير الشبكة هاكراً مشابهاً وعلى علم بهذه الاحتيالات ودائما ما يراقب شبكته والرسائل القادمة إليها والحقيقة أن الكثير من الشركات يحلم بمثل مدير الشبكة هذا ولكن الخوف أن يكون «حاميها حراميها».وللحديث بقية مع الشبكات اللاسلكية.

Shortcut فيروس في رسالة وفيروس في الرسالة التالية هذا ما احتواه صندوق البريد في فترة نهاية السنة الميلادية وحقا إنه موسم الفيروسات وكل فيروس وأنت بخير.

يبدو أن الحديث عن الهاكرز والحماية يغضب البعض ممن لا يريدون للآخرين معرفة الحقيقة لكيلا يكشفوا عيوبا يحاولون إخفاءها بكل جهدهم.

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com

الإنترنت المجانية في مصر حلم الكثير من مستخدمي الشبكة العنكبوتية في المملكة ولكن المتفائلين منهم يطالبون على الأقل بتخفيض تسعيرة المكالمات الهاتفية الخاصة بالإنترنت.. فهل من مستمع؟
الثغرات في أنظمة التشغيل ليست حكرا على ويندوز **XP** ولكن الحملة الدعائية لمايكروسوفت يبدو أنها السبب في تضخيم أمر اكتشاف الثغرات مما جعل الكثيرين يتخوفون من استخدام نظام التشغيل المذكور

الموضوع الثلاثين : طريقة لتثبيت الويندوز بدون Number Serial

طريقة لتثبيت الويندوز بدون **Serial Number** وهي كالتالي :
أولا : قم بنسخ ملفات جميع ملفات الويندوز من القرص المدمج الى الهارد ديسك وضعه في مجلد خاص وليكن مثلا : **D:\win98** .
ثانيا : ابحث عن الملف التالي : **PRECOPY2.zip** ضمن المجلد **D:\win98** الذي أنشأته للتو ووضعت فيه ملفات الويندوز .
ثالثا : افتح هذا الملف من خلال الوين زيب ثم ابحث عن الملف **setupx.dll** وفك ضغطه في ملف المجلد الذي نسخت اليه ملفات الويندوز مثال : **D:\Win98\setupx.dll**
رابعا : افتح هذا الملف باستخدام البرنامج التالي : **exescope** وتجده في هنا :
http://windows.online.pl/pliki/exescope.zip حجمه : 413 **k.b**
خامسا : سيفتح لك البرنامج هذا الملف ثم من خلال **Resource** افتح **String** وابحث عن رقم 34 ثم اضغط عليه ،
الآن سيظهر لك (يمينا) رقم هو 530.1 قم بتعديله الى 530.0 ثم احفظ الملف .
والآن عندما يطلب منك الويندوز سيريال نمبر اكتي أي شي .

مع اجمل تحياتي وخالص احترامي لمن تعاون واحدث وكتب هذا الكم الهائل من المعلومات المهمة،،،

اعداد سيف علي حسن الدار

سيف علي حسن الدار
+967/ 771323146 -735446181
aldare-1989@hotmail.Com
saif201028@yahoo.com